

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-136231

(43)Date of publication of application : 21.05.1999

(51)Int.Cl.

H04L 9/14

G09C 1/00

(21)Application number : 10-222656

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD

(22)Date of filing : 06.08.1998

(72)Inventor : TATEBAYASHI MAKOTO

(30)Priority

Priority number : 09211507

Priority date : 06.08.1997

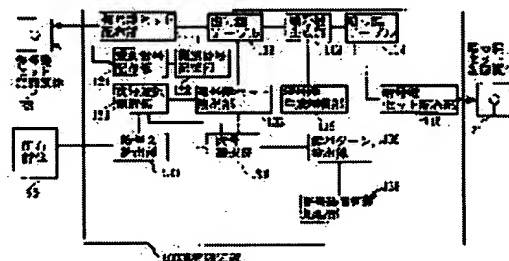
Priority country : JP

(54) ENCRYPTION KEY

(57)Abstract:

PROBLEM TO BE SOLVED: To provide the encryption system where from which kind of an encryption device a distribution medium is produced is identified.

SOLUTION: A decoding selection control section 131 controls an encrypted text read section 133, a decoding key set read section 132, a decoding selection section 134 to repetitively read an encrypted scramble key, to read a decoding key set, and to decode the read scrambled key. As a result, N-sets of keys used to decode N-sets of decoding texts including decoded scramble keys are selected. A key pattern detection section 135 detects one encryption key set coincident with the N-sets of selected key sets among M-sets of encryption key sets stored in an encryption key table 114.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision]

BEST AVAILABLE COPY

of rejection]

[Date of requesting appeal against examiner's
decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(11)特許出願公開番号

特開平11-136231

(43)公開日 平成11年(1999)5月21日

(51) Int.Cl.⁸

識別記号

FI

H04L 9/14

H0 4 L 9/00

641

G O 9 C 1/00

G O 9 C 1/00

6 6 0 D

660

審査請求 未請求 請求項の数40 O.L (全 31 頁)

(21)出願番号 特願平10-222656

(22)出願日 平成10年(1998)8月6日

(31) 優先権主張番号 特願平9-211507

(32)優先日 平9(1997)8月6日

(33)優先権主張国 日本 (JP)

(71)出願人 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(72)発明者 館林 誠

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

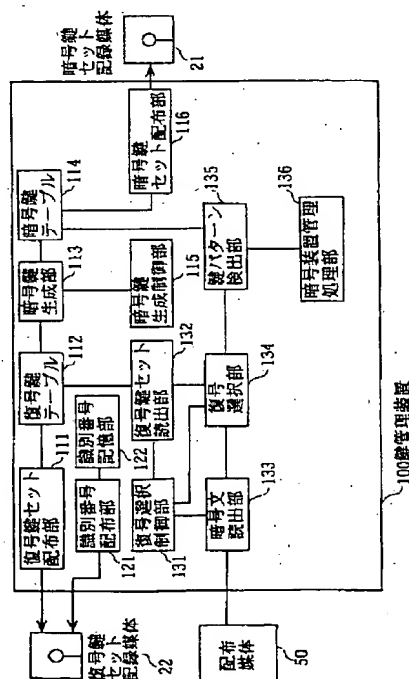
(74)代理人 弁理士 中島 司朗 (外1名)

(54) 【発明の名称】 暗号システム

(57) 【要約】

【課題】 配布媒体がどの種類の暗号装置により生産されたものであるかを識別することのできる暗号システムを提供することを目的とする。

【解決手段】 復号選択制御部 131 は、暗号文読出部 133 と、復号鍵セット読出部 132 と、復号選択部 134 とに対して、暗号化スクランブルキーの読み出しと、復号鍵セットの読み出しと、読み出した暗号化スクランブルキーの復号とを繰り返すよう制御する。この結果、N 個の復号されたスクランブルキーを含む復号文が復号される際に用いられた N 個の鍵のセットが選択される。鍵パターン検出部 135 は、暗号鍵テーブル 114 に記憶されている M 個の暗号鍵セットから、前記選択された N 個の鍵のセットと一致する 1 つの暗号鍵セットを検出する。



【特許請求の範囲】

【請求項 1】 1 台の鍵管理装置と、M (M は 2 以上の整数) 種類の暗号装置と、N (N は 2 以上の整数) 種類の復号装置とからなる暗号システムであって、前記鍵管理装置は、復号鍵セットを N 個記憶し、暗号鍵セットを M 個記憶し、N 個の識別番号を記憶し、前記 M 個の暗号鍵セットをそれぞれ前記 M 種類の暗号装置に配布し、前記 N 個の復号鍵セットをそれぞれ前記 N 種類の復号装置に配布し、前記 N 個の識別番号をそれぞれ前記 N 種類の復号装置に配布し、前記暗号鍵セットは N 個の暗号鍵からなり、前記復号鍵セットは所定数の復号鍵からなり、前記 M 種類の暗号装置のそれぞれは、デジタルデータをスクランブルキーを用いて暗号化して暗号化デジタルデータを生成し、前記配布された暗号鍵セットを用いて前記スクランブルキーを暗号化して N 個の暗号化スクランブルキーを生成し、前記暗号化デジタルデータと前記 N 個の暗号化スクランブルキーとを配布媒体に書き込み、前記 N 種類の復号装置のそれぞれは、前記配布された復号鍵セットに含まれる前記所定数の復号鍵を用いて、前記配布媒体に含まれる前記配布された識別番号により特定される 1 つの暗号化スクランブルキーを順次復号し、第 1 の所定の基準により正しく復号されたスクランブルキーを用いて前記配布媒体に含まれる暗号化デジタルデータを復号してデジタルデータを生成し、識別番号は、配布媒体に書き込まれている N 個の暗号化スクランブルキーから当該復号装置に対応する 1 つの暗号化スクランブルキーを識別し、前記鍵管理装置は、さらに、前記配布媒体から 1 つの暗号化スクランブルキーを読み出す第 1 暗号文読出手段と、1 つの復号鍵セットを読み出す復号鍵セット読出手段と、前記読み出した復号鍵セットに含まれる前記所定数の復号鍵を用いて、前記読み出した暗号化スクランブルキーを順次復号し、前記第 1 の所定の基準により正しく暗号化スクランブルキーを復号する復号鍵を、前記所定数の復号鍵の中から 1 つ選択する復号鍵選択手段と、前記配布媒体から N 個の暗号化スクランブルキーの読み出しが終了するまで、前記第 1 暗号文読出手段、前記復号鍵セット読出手段、前記復号鍵選択手段に対して、暗号化スクランブルキーの読み出しと、復号鍵セットの読み出しと、読み出した暗号化スクランブルキーの復号とを繰り返し行うように制御し、その結果 N 個の復号鍵のセットが選択される第 1 繰返制御手段と、前記 M 個の暗号鍵セットから、前記選択された N 個の復号鍵のセットと一致する 1 つの暗号鍵セットを検出し、検出された暗号鍵セットにより特定される暗号装置を識別する鍵パターン検出手段とを備えることを特徴とする暗号システム。

【請求項 2】 前記鍵管理装置は、

所定数の復号鍵からなる復号鍵セットを N 個記憶している第 1 復号鍵記憶手段と、前記第 1 復号鍵記憶手段に記憶されている N 個の復号鍵セットのそれぞれから、第 1 の所定の方法により 1 つの復号鍵を選択して 1 つの暗号鍵とし、N 個の暗号鍵からなる暗号鍵セットを生成する暗号鍵生成手段と、前記生成された 1 つの暗号鍵セットを記憶する第 1 暗号鍵記憶手段と、M 個の暗号鍵セットが生成されるまで、前記暗号鍵生成手段に対して、暗号鍵セットの生成を繰り返すように制御し、その結果、前記第 1 暗号鍵記憶手段は M 個の暗号鍵セットを記憶する第 2 繰返制御手段と、前記第 1 暗号鍵記憶手段に記憶されている M 個の暗号鍵セットをそれぞれ前記 M 種類の暗号装置に配布する暗号鍵セット配布手段と、前記第 1 復号鍵記憶手段に記憶されている N 個の復号鍵セットをそれぞれ前記 N 種類の復号装置に配布する復号鍵セット配布手段と、N 個の識別番号をそれぞれ前記 N 種類の復号装置に配布する識別番号配布手段とを備えることを特徴とする請求項 1 記載の暗号システム。

【請求項 3】 前記第 1 の所定の方法とは、前記第 1 復号鍵記憶手段に記憶されている N 個の復号鍵セットのそれぞれから、ランダムに 1 個の復号鍵を選択することであることを特徴とする請求項 2 記載の暗号システム。

【請求項 4】 前記第 1 の所定の方法とは、前記第 1 復号鍵記憶手段に記憶されている N 個の復号鍵セットのそれぞれから、一様にランダムに 1 個の復号鍵を選択することであることを特徴とする請求項 2 記載の暗号システム。

【請求項 5】 前記 M 種類の暗号装置のそれぞれは、前記鍵管理装置から配布された 1 つの暗号鍵セットを受信し、受信した前記暗号鍵セットを記憶する第 2 暗号鍵記憶手段と、スクランブルキーを生成するスクランブルキー生成手段と、外部からデジタルデータを受信し、受信したデジタルデータを前記生成されたスクランブルキーを用いて暗号化し、暗号化デジタルデータを生成するデジタルデータ暗号化手段と、前記第 2 暗号鍵記憶手段に記憶されている暗号鍵セットに含まれる N 個の暗号鍵を用いて、第 2 の所定の方法により、前記スクランブルキーを順次暗号化し、N 個の暗号化スクランブルキーを生成する鍵暗号化手段と、前記生成された暗号化デジタルデータと前記生成された N 個の暗号化スクランブルキーとを配布媒体に書き込み、媒体書込手段とを備えることを特徴とする請求項 1 記載の暗号システム。

【請求項 6】 前記第 2 の所定の方法とは、前記スクラ

ンブルキーと固定値からなる固定情報とを結合し、結合されたスクランブルキーと固定情報とを暗号化することであることを特徴とする請求項 5 記載の暗号システム。

【請求項 7】 前記第 2 の所定の方法とは、前記スクランブルキーを暗号化して N 個の暗号化スクランブルキーを生成し、さらに、固定値からなる固定情報を暗号化して N 個の暗号化固定情報を生成することであり、前記媒体書込手段は、暗号化デジタルデータと N 個の暗号化スクランブルキーと N 個の暗号化固定情報とを配布媒体に書き込むことを特徴とする請求項 5 記載の暗号システム。

【請求項 8】 前記復号選択手段は、前記復号鍵セットから復号鍵を順次読み出す第 1 復号鍵読出手段と、前記読み出した復号鍵を用いて、前記読み出した暗号化スクランブルキーを復号し、復号文を生成する第 1 復号文生成手段と、前記第 1 の所定の基準により、復号文が正しく復号されているかどうかを検査する第 1 復号文検査手段と、前記復号鍵セットから所定数の復号鍵の読出しが終了するまで、前記第 1 復号鍵読出手段、前記第 1 復号文生成手段、前記第 1 復号文検査手段に対して、復号鍵の読出しと、暗号化スクランブルキーの復号と、復号文の検査とを繰り返し行うように制御する第 3 繰返制御手段と、前記復号文検査手段により正しく復号されたと検査された際に用いられた復号鍵を出力する鍵出力手段とを備えることを特徴とする請求項 1 記載の暗号システム。

【請求項 9】 前記第 1 の所定の基準とは、前記復号文に固定値からなる固定情報が含まれることであることを特徴とする請求項 8 記載の暗号システム。

【請求項 10】 前記配布媒体は、さらに、前記暗号鍵セットに含まれる N 個の暗号鍵を用いて固定値からなる固定情報が暗号化された N 個の暗号化固定情報を含み、前記鍵管理装置は、さらに、N 個の暗号化固定情報を読み出す暗号化固定情報読出手段と、前記 N 個の復号鍵セットを用いて、前記読み出した N 個の暗号化固定情報をそれぞれ復号する暗号化固定情報復号手段とを含み、

前記第 1 の所定の基準とは、暗号化固定情報を復号して復号文を生成し、生成された復号文に固定値からなる固定情報が含まれることであることを特徴とする請求項 8 記載の暗号システム。

【請求項 11】 前記 N 種類の復号装置のそれぞれは、前記鍵管理装置から識別番号を受信し、受信した識別番号を記憶する識別番号記憶手段と、前記鍵管理装置から配布された 1 つの復号鍵セットを受信し、受信した前記復号鍵セットを記憶する第 2 復号鍵記憶手段と、前記配布媒体から前記受信した識別番号により識別され

る 1 つの暗号化スクランブルキーを読み出す第 2 暗号文読出手段と、

前記配布媒体から暗号化デジタルデータを読み出すデジタルデータ読出手段と、

前記第 2 復号鍵記憶手段から前記復号鍵セットに含まれる復号鍵を順次読み出す第 2 復号鍵読出手段と、

前記読み出した復号鍵を用いて、前記読み出した暗号化スクランブルキーを復号し、復号文を生成する第 2 復号文生成手段と、

前記第 1 の所定の基準により、復号文が正しく復号されているかどうかを検査し、正しく復号された場合に前記復号文をスクランブルキーとする第 2 復号文検査手段と、

復号鍵セットから所定数の復号鍵の読出しが終了するまで、前記第 2 復号鍵読出手段、前記第 2 復号文生成手段、前記第 2 復号文検査手段に対して、復号鍵の読出しと、暗号化スクランブルキーの復号と、復号文の検査とを繰り返し行うように制御する第 4 繰返制御手段と、

前記復号文検査手段により正しく復号されたと検査されたスクランブルキーを用いて、前記読み出した暗号化デジタルデータを復号し、デジタルデータを生成するデジタルデータ復号手段とを備えることを特徴とする請求項 1 記載の暗号システム。

【請求項 12】 前記第 1 の所定の基準とは、前記復号文に固定値からなる固定情報が含まれることであることを特徴とする請求項 1 1 記載の暗号システム。

【請求項 13】 前記配布媒体は、さらに、前記暗号鍵セットに含まれる N 個の暗号鍵を用いて固定値からなる固定情報が暗号化された N 個の暗号化固定情報を含み、前記復号装置は、さらに、

前記識別番号により識別される 1 つの暗号化固定情報を読み出す暗号化固定情報読出手段と、

前記復号鍵セットに含まれる所定数の復号鍵を用いて、前記読み出した暗号化固定情報を復号する暗号化固定情報復号手段とを備え、

前記第 1 の所定の基準とは、暗号化固定情報を復号して復号文を生成し、生成された復号文に固定値からなる固定情報が含まれることであることを特徴とする請求項 1 1 記載の暗号システム。

【請求項 14】 前記 M 種類の暗号装置のそれぞれは、前記鍵管理装置から配布された 1 つの暗号鍵セットを受信し、受信した前記暗号鍵セットを記憶する第 2 暗号鍵記憶手段と、

スクランブルキーを生成するスクランブルキー生成手段と、

外部からデジタルデータを受信し、受信したデジタルデータを前記生成されたスクランブルキーを用いて暗号化し、暗号化デジタルデータを生成するデジタルデータ暗号化手段と、

前記第 2 暗号鍵記憶手段に記憶されている暗号鍵セット

に含まれるN個の暗号鍵を用いて、第2の所定の方法により、前記スクランブルキーを順次暗号化し、N個の暗号化スクランブルキーを生成する鍵暗号化手段と、前記生成された暗号化デジタルデータと前記生成されたN個の暗号化スクランブルキーとを配布媒体に書き込む媒体書込手段とを備え、

前記鍵管理装置において、前記復号選択手段は、前記復号鍵セットから復号鍵を順次読み出す第1復号鍵読出手段と、

前記読み出した復号鍵を用いて、前記読み出した暗号化スクランブルキーを復号し、復号文を生成する第1復号文生成手段と、
前記第1の所定の基準により、復号文が正しく復号されているかどうかを検査する第1復号文検査手段と、
前記復号鍵セットから所定数の復号鍵の読出しが終了するまで、前記第1復号鍵読出手段、前記第1復号文生成手段、前記第1復号文検査手段に対して、復号鍵の読出しと、暗号化スクランブルキーの復号と、復号文の検査とを繰り返し行うように制御する第3繰返制御手段と、
前記復号文検査手段により正しく復号されたと検査された際に用いられた復号鍵を出力する鍵出力手段とを備えることを特徴とする請求項1記載の暗号システム。

【請求項15】 前記第1の所定の基準とは、前記復号文に固定情報が含まれることであり、

前記第2の所定の方法とは、前記スクランブルキーと固定値からなる固定情報とを結合し、結合されたスクランブルキーと固定情報とを暗号化することであることを特徴とする請求項14記載の暗号システム。

【請求項16】 前記第2の所定の方法とは、前記スクランブルキーを暗号化してN個の暗号化スクランブルキーを生成し、さらに、固定値からなる固定情報を暗号化してN個の暗号化固定情報を生成することであり、
前記媒体書込手段は、暗号化デジタルデータとN個の暗号化スクランブルキーとN個の暗号化固定情報とを配布媒体に書き込み、

前記鍵管理装置は、
N個の暗号化固定情報を読み出す暗号化固定情報読出手段と、

N個の復号鍵セットを用いて、前記読み出したN個の暗号化固定情報をそれぞれ復号する暗号化固定情報復号手段とを備え、

前記第1の所定の基準とは、N個の暗号化固定情報を復号し、さらに、固定情報を生成することであることを特徴とする請求項14記載の暗号システム。

【請求項17】 前記M種類の暗号装置のそれぞれは、
前記鍵管理装置から配布された1つの暗号鍵セットを受信し、受信した前記暗号鍵セットを記憶する第2暗号鍵記憶手段と、

スクランブルキーを生成するスクランブルキー生成手段と、

外部からデジタルデータを受信し、受信したデジタルデータを前記生成されたスクランブルキーを用いて暗号化し、暗号化デジタルデータを生成するデジタルデータ暗号化手段と、

前記第2暗号鍵記憶手段に記憶されている暗号鍵セットに含まれるN個の暗号鍵を用いて、第2の所定の方法により、前記スクランブルキーを順次暗号化し、N個の暗号化スクランブルキーを生成する鍵暗号化手段と、

前記生成された暗号化デジタルデータと前記生成されたN個の暗号化スクランブルキーとを配布媒体に書き込む媒体書込手段とを備え、

前記N種類の復号装置のそれぞれは、

前記鍵管理装置から識別番号を受信し、受信した識別番号を記憶する識別番号記憶手段と、

前記鍵管理装置から配布された1つの復号鍵セットを受信し、受信した前記復号鍵セットを記憶する第2復号鍵記憶手段と、

前記配布媒体から前記受信した識別番号により識別される1つの暗号化スクランブルキーを読み出す第2暗号文読出手段と、

前記配布媒体から暗号化デジタルデータを読み出すデジタルデータ読出手段と、

前記第2復号鍵記憶手段から前記復号鍵セットに含まれる復号鍵を順次読み出す第2復号鍵読出手段と、

前記読み出した復号鍵を用いて、前記読み出した暗号化スクランブルキーを復号し、復号文を生成する第2復号文生成手段と、

前記第1の所定の基準により、復号文が正しく復号されているかどうかを検査し、正しく復号された場合に前記復号文はスクランブルキーを含む第2復号文検査手段と、

復号鍵セットから所定数の復号鍵の読出しが終了するまで、前記第2復号鍵読出手段、前記第2復号文生成手段、前記第2復号文検査手段に対して、復号鍵の読出しと、暗号化スクランブルキーの復号と、復号文の検査とを繰り返し行うように制御する第4繰返制御手段と、

前記復号文検査手段により正しく復号されたと検査されたスクランブルキーを用いて、前記読み出した暗号化デジタルデータを復号し、デジタルデータを生成するデジタルデータ復号手段とを備えることを特徴とする請求項1記載の暗号システム。

【請求項18】 前記第1の所定の基準とは、前記復号文に固定情報が含まれることであり、

前記第2の所定の方法とは、前記スクランブルキーと固定値からなる固定情報とを結合し、結合されたスクランブルキーと固定情報とを暗号化することであることを特徴とする請求項17記載の暗号システム。

【請求項19】 前記第2の所定の方法とは、前記スクランブルキーを暗号化してN個の暗号化スクランブルキーを生成し、さらに、固定値からなる固定情報を暗号化

してN個の暗号化固定情報を生成することであり、
前記媒体書込手段は、暗号化デジタルデータとN個の暗号化スクランブルキーとN個の暗号化固定情報とを配布媒体に書き込み、

前記復号装置は、さらに、

前記識別番号により識別される暗号化固定情報を読み出す暗号化固定情報読出手段と、

復号鍵セットに含まれる所定数の復号鍵を用いて、前記読み出した暗号化固定情報を読み出す暗号化固定情報復号手段とを備え、

前記第1の所定の基準とは、暗号化固定情報を復号し、さらに、固定情報を生成することであることを特徴とする請求項17記載の暗号システム。

【請求項20】 前記鍵管理装置は、

所定数の復号鍵からなる復号鍵セットをN個記憶している第1復号鍵記憶手段と、

前記第1復号鍵記憶手段に記憶されているN個の復号鍵セットのそれぞれから、第1の所定の方法により1つの復号鍵を選択して1つの暗号鍵とし、N個の暗号鍵からなる暗号鍵セットを生成する暗号鍵生成手段と、

前記生成された1つの暗号鍵セットを記憶する第1暗号鍵記憶手段と、

M個の暗号鍵セットが生成されるまで、前記暗号鍵生成手段に対して、暗号鍵セットの生成を繰り返すように制御し、この結果、前記第1暗号鍵記憶手段はM個の暗号鍵セットを記憶する第2繰返制御手段と、

前記第1暗号鍵記憶手段に記憶されているM個の暗号鍵セットをそれぞれ前記M種類の暗号装置に配布する暗号鍵セット配布手段と、

前記第1復号鍵記憶手段に記憶されているN個の復号鍵セットをそれぞれ前記N種類の復号装置に配布する復号鍵セット配布手段と、

識別番号を前記N種類の復号装置に配布する識別番号配布手段とを備え、

前記N種類の復号装置のそれぞれは、

前記鍵管理装置から識別番号を受信し、受信した識別番号を記憶する識別番号記憶手段と、

前記鍵管理装置から配布された1つの復号鍵セットを受信し、受信した前記復号鍵セットを記憶する第2復号鍵記憶手段と、

前記配布媒体から前記受信した識別番号により識別される1つの暗号化スクランブルキーを読み出す第2暗号文読出手段と、

前記配布媒体から暗号化デジタルデータを読み出すデジタルデータ読出手段と、

前記第2復号鍵記憶手段から前記復号鍵セットに含まれる復号鍵を順次読み出す第2復号鍵読出手段と、

前記読み出した復号鍵を用いて、前記読み出した暗号化スクランブルキーを復号し、復号文を生成する第2復号文生成手段と、

前記第1の所定の基準により、復号文が正しく復号されているかどうかを検査し、正しく復号された場合に前記復号文をスクランブルキーとする第2復号文検査手段と、

復号鍵セットから所定数の復号鍵の読出しが終了するまで、前記第2復号鍵読出手段、前記第2復号文生成手段、前記第2復号文検査手段に対して、復号鍵の読出しと、暗号化スクランブルキーの復号と、復号文の検査とを繰り返し行うように制御する第4繰返制御手段と、

10 前記復号文検査手段により正しく復号されたと検査されたスクランブルキーを用いて、前記読み出した暗号化デジタルデータを復号し、デジタルデータを生成するデジタルデータ復号手段とを備えることを特徴とする請求項1記載の暗号システム。

【請求項21】 前記第1の所定の方法とは、前記第1復号鍵記憶手段に記憶されているN個の復号鍵セットのそれぞれから、ランダムに1個の復号鍵を選択することであることを特徴とする請求項20記載の暗号システム。

20 【請求項22】 前記第1の所定の方法とは、前記第1復号鍵記憶手段に記憶されているN個の復号鍵セットのそれぞれから、一様にランダムに1個の復号鍵を選択することであることを特徴とする請求項20記載の暗号システム。

【請求項23】 前記第1の所定の基準とは、前記復号文に固定値からなる固定情報が含まれることであることを特徴とする請求項20記載の暗号システム。

【請求項24】 前記配布媒体は、さらに、前記暗号鍵セットに含まれるN個の暗号鍵を用いて固定値からなる固定情報が暗号化されたN個の暗号化固定情報を含み、前記復号装置は、さらに、前記識別番号により識別される1つの暗号化固定情報を読み出す暗号化固定情報読出手段と、前記復号鍵セットに含まれる所定数の復号鍵を用いて、前記読み出した暗号化固定情報を復号する暗号化固定情報復号手段とを備え、

40 前記第1の所定の基準とは、暗号化固定情報を復号して復号文を生成し、生成された復号文に固定値からなる固定情報が含まれることであることを特徴とする請求項20記載の暗号システム。

【請求項25】 M (Mは2以上の整数) 種類の暗号装置とN (Nは2以上の整数) 種類の復号装置に鍵情報を配布する鍵管理装置であって、

所定数の復号鍵からなる復号鍵セットをN個記憶している復号鍵記憶手段と、

前記復号鍵記憶手段に記憶されているN個の復号鍵セットのそれぞれから、第1の所定の方法により1つの復号鍵を選択して1つの暗号鍵とし、N個の暗号鍵からなる暗号鍵セットを生成する暗号鍵生成手段と、

50 前記生成された1つの暗号鍵セットを記憶する暗号鍵記

憶手段と、

M個の暗号鍵セットが生成されるまで、前記暗号鍵生成手段に対して、暗号鍵セットの生成を繰り返すように制御し、その結果、前記暗号鍵記憶手段はM個の暗号鍵セットを記憶する繰返制御手段と、

前記第1暗号鍵記憶手段に記憶されているM個の暗号鍵セットをそれぞれM種類の暗号装置に配布する暗号鍵セット配布手段と、

前記第1復号鍵記憶手段に記憶されているN個の復号鍵セットをそれぞれN種類の復号装置に配布する復号鍵セット配布手段と、

N個の識別番号をそれぞれN種類の復号装置に配布する識別番号配布手段とを備えることを特徴とする鍵管理装置。

【請求項26】 鍵管理装置から配布される鍵情報を用いて、デジタルデータを暗号化して配布媒体に書き込む暗号装置であって、

鍵管理装置から配布された1つの暗号鍵セットを受信し、受信した前記暗号鍵セットを記憶する暗号鍵記憶手段と、

スクランブルキーを生成するスクランブルキー生成手段と、

外部からデジタルデータを受信し、受信したデジタルデータを前記生成されたスクランブルキーを用いて暗号化し、暗号化デジタルデータを生成するデジタルデータ暗号化手段と、

前記暗号鍵記憶手段に記憶されている暗号鍵セットに含まれるN(Nは2以上の整数)個の暗号鍵を用いて、所定の方法により、前記スクランブルキーを順次暗号化し、N個の暗号化スクランブルキーを生成する鍵暗号化手段と、

前記生成された暗号化デジタルデータと前記生成されたN個の暗号化スクランブルキーとを配布媒体に書き込む媒体書込手段とを備えることを特徴とする暗号装置。

【請求項27】 鍵管理装置から配布された鍵情報を用いて、配布媒体に書かれた暗号化デジタルデータを復号する復号装置であって、

配布媒体に書き込まれているN個の暗号化スクランブルキーから当該復号装置に対応する1つの暗号化スクランブルキーを識別する識別番号を鍵管理装置から受信し、受信した識別番号を記憶する識別番号記憶手段と、

鍵管理装置から配布された1つの復号鍵セットを受信し、受信した前記復号鍵セットを記憶する復号鍵記憶手段と、

前記配布媒体から前記受信した識別番号により識別される1つの暗号化スクランブルキーを読み出す暗号文読出手段と、

前記配布媒体から暗号化デジタルデータを読み出すデジタルデータ読出手段と、

前記復号鍵記憶手段から前記復号鍵セットに含まれる復

号鍵を順次読み出す復号鍵読出手段と、

前記読み出した復号鍵を用いて、前記読み出した暗号化スクランブルキーを復号し、復号文を生成する復号文生成手段と、

所定の基準により、復号文が正しく復号されているかどうかを検査し、正しく復号された場合に前記復号文はスクランブルキーを含む復号文検査手段と、

復号鍵セットから所定数の復号鍵の読出しが終了するまで、前記復号鍵読出手段、前記復号文生成手段、前記復号文検査手段に対して、復号鍵の読出しと、暗号化スクランブルキーの復号と、復号文の検査とを繰り返し行うように制御する繰返制御手段と、

前記復号文検査手段により正しく復号されたと検査されたスクランブルキーを用いて、前記読み出した暗号化デジタルデータを復号し、デジタルデータを生成するデジタルデータ復号手段とを備えることを特徴とする復号装置。

【請求項28】 配布媒体にデジタルデータを暗号化して書き込んだ暗号装置の種類を識別する鍵管理装置であって、

前記配布媒体から1つの暗号化スクランブルキーを読み出す暗号文読出手段と、

1つの復号鍵セットを読み出す復号鍵セット読出手段と、

前記読み出した復号鍵セットに含まれる所定数の復号鍵を用いて、前記読み出した暗号化スクランブルキーを順次復号し、所定の基準により正しく暗号化スクランブルキーを復号する復号鍵を、前記所定数の復号鍵の中から1つ選択する復号選択手段と、

前記配布媒体からN個の暗号化スクランブルキーの読出しが終了するまで、前記暗号文読出手段、前記復号鍵セット読出手段、前記復号選択手段に対して、暗号化スクランブルキーの読み出しと、復号鍵セットの読み出しと、読み出した暗号化スクランブルキーの復号とを繰り返し行うように制御し、この結果、N個の復号鍵のセットが選択される繰返制御手段と、

前記M個の暗号鍵セットから、前記選択されたN個の復号鍵のセットと一致する1つの暗号鍵セットを検出し、検出された暗号鍵セットにより特定される暗号装置を識別する鍵パターン検出手段とを備えることを特徴とする鍵管理装置。

【請求項29】 M(Mは2以上の整数)種類の暗号装置とN(Nは2以上の整数)種類の復号装置に鍵情報を配布し、所定数の復号鍵からなる復号鍵セットをN個記憶している復号鍵記憶手段を備える鍵管理装置において用いられる鍵管理方法であって、

前記復号鍵記憶手段に記憶されているN個の復号鍵セットのそれぞれから、所定の方法により1つの復号鍵を選択して1つの暗号鍵とし、N個の暗号鍵からなる暗号鍵セットを生成する暗号鍵生成ステップと、

M個の暗号鍵セットが生成されるまで、前記暗号鍵生成ステップに対して、暗号鍵セットの生成を繰り返すように制御し、この結果、M個の暗号鍵セットが生成される繰返制御ステップと、

暗号鍵生成ステップにより生成されたM個の暗号鍵セットをそれぞれM種類の暗号装置に配布する暗号鍵セット配布ステップと、

前記復号鍵記憶手段に記憶されているN個の復号鍵セットをそれぞれN種類の復号装置に配布する復号鍵セット配布ステップと、

N個の識別番号をそれぞれN種類の復号装置に配布する識別番号配布ステップとを含むことを特徴とする鍵管理方法。

【請求項30】 前記所定の方法とは、前記復号鍵記憶手段に記憶されているN個の復号鍵セットのそれぞれから、ランダムに1個の復号鍵を選択することであることを特徴とする請求項29記載の鍵管理方法。

【請求項31】 前記所定の方法とは、前記復号鍵記憶手段に記憶されているN個の復号鍵セットのそれぞれから、一様にランダムに1個の復号鍵を選択することであることを特徴とする請求項29記載の鍵管理方法。

【請求項32】 鍵管理装置から配布される鍵情報を用いて、デジタルデータを暗号化して配布媒体に書き込み、鍵管理装置から配布された1つの暗号鍵セットを受信し受信した前記暗号鍵セットを記憶する暗号鍵記憶手段を備える暗号装置において用いられる暗号方法であって、

スクランブルキーを生成するスクランブルキー生成ステップと、

外部からデジタルデータを受信し、受信したデジタルデータを前記生成されたスクランブルキーを用いて暗号化し、暗号化デジタルデータを生成するデジタルデータ暗号化ステップと、

前記暗号鍵記憶手段に記憶されている暗号鍵セットに含まれるN（Nは2以上の整数）個の暗号鍵を用いて、所定の方法により、前記スクランブルキーを順次暗号化し、N個の暗号化スクランブルキーを生成する鍵暗号化ステップと、

前記生成された暗号化デジタルデータと前記生成されたN個の暗号化スクランブルキーとを配布媒体に書き込む媒体書込ステップとを含むことを特徴とする暗号方法。

【請求項33】 前記所定の方法とは、前記スクランブルキーと固定値からなる固定情報とを結合し、結合されたスクランブルキーと固定情報とを暗号化することであることを含むことを特徴とする請求項32記載の暗号方法。

【請求項34】 前記所定の方法とは、前記スクランブルキーを暗号化してN個の暗号化スクランブルキーを生成し、さらに、固定値からなる固定情報を暗号化してN個の暗号化固定情報を生成することであり、

前記媒体書込ステップは、暗号化デジタルデータとN個

の暗号化スクランブルキーとN個の暗号化固定情報とを配布媒体に書き込むことを特徴とする請求項32記載の暗号方法。

【請求項35】 鍵管理装置から配布された鍵情報を用いて、配布媒体に書かれた暗号化デジタルデータを復号し、鍵管理装置から識別番号を受信し受信した識別番号を記憶する識別番号記憶手段と、鍵管理装置から配布された1つの復号鍵セットを受信し受信した前記復号鍵セットを記憶する復号鍵記憶手段とを備える復号装置において用いられる復号方法であって、

前記識別番号は配布媒体に書き込まれているN個の暗号化スクランブルキーから当該復号装置に対応する1つの暗号化スクランブルキーを識別し、

前記配布媒体から前記受信した識別番号により識別される1つの暗号化スクランブルキーを読み出す暗号文読出ステップと、

前記配布媒体から暗号化デジタルデータを読み出すデジタルデータ読出ステップと、

前記復号鍵記憶手段から前記復号鍵セットに含まれる復号鍵を順次読み出す復号鍵読出ステップと、

前記読み出した復号鍵を用いて、前記読み出した暗号化スクランブルキーを復号し、復号文を生成する復号文生成ステップと、

所定の基準により、復号文が正しく復号されているかどうかを検査し、正しく復号された場合に前記復号文はスクランブルキーを含む復号文検査ステップと、

復号鍵セットから所定数の復号鍵の読出しが終了するまで、前記復号鍵読出ステップ、前記復号文生成ステップ、前記復号文検査ステップに対して、復号鍵の読出しと、暗号化スクランブルキーの復号と、復号文の検査とを繰り返すように制御する繰返制御ステップと、前記復号文検査ステップにより正しく復号されたと検査されたスクランブルキーを用いて、前記読み出した暗号化デジタルデータを復号し、デジタルデータを生成するデジタルデータ復号ステップとを含むことを特徴とする復号方法。

【請求項36】 前記所定の基準とは、前記復号文に固定値からなる固定情報が含まれることであることを特徴とする請求項35記載の復号方法。

【請求項37】 前記配布媒体は、さらに、暗号鍵セットに含まれるN個の暗号鍵を用いて固定値からなる固定情報が暗号化されたN個の暗号化固定情報を含み、

前記復号方法は、さらに、

前記識別番号により識別される1つの暗号化固定情報を読み出す暗号化固定情報読出ステップと、

復号鍵セットに含まれる所定数の復号鍵を用いて、前記読み出した暗号化固定情報を復号する暗号化固定情報復号ステップとを含み、

前記所定の基準とは、暗号化固定情報を復号して復号文を生成し、生成された復号文に固定値からなる固定情報

が含まれることであることを特徴とする請求項 3 5 記載の復号方法。

【請求項 3 8】 配布媒体にデジタルデータを暗号化して書き込んだ暗号装置の種類を識別する鍵管理装置において用いられる鍵管理方法であって、
前記配布媒体から 1 つの暗号化スクランブルキーを読み出す暗号文読出ステップと、
1 つの復号鍵セットを読み出す復号鍵セット読出ステップと、
前記読み出した復号鍵セットに含まれる所定数の復号鍵を用いて、前記読み出した暗号化スクランブルキーを順次復号し、所定の基準により正しく暗号化スクランブルキーを復号する復号鍵を、前記所定数の復号鍵の中から 1 つ選択する復号選択ステップと、
前記配布媒体から N (N は 2 以上の整数) 個の暗号化スクランブルキーの読み出しが終了するまで、前記暗号文読出ステップ、前記復号鍵セット読出ステップ、前記復号選択ステップに対して、暗号化スクランブルキーの読み出しと、復号鍵セットの読み出しと、読み出した暗号化スクランブルキーの復号とを繰り返し行うように制御し、この結果、N 個の復号鍵のセットが選択される繰返制御ステップと、
前記 M 個の暗号鍵セットから、前記選択された N 個の復号鍵のセットと一致する 1 つの暗号鍵セットを検出し、検出された暗号鍵セットにより特定される暗号装置の種類を識別する鍵パターン検出ステップとを含むことを特徴とする鍵管理方法。

【請求項 3 9】 前記所定の基準とは、前記復号文に固定値からなる固定情報が含まれることであることを特徴とする請求項 3 8 記載の鍵管理方法。

【請求項 4 0】 前記配布媒体は、さらに、暗号鍵セットに含まれる N 個の暗号鍵を用いて固定値からなる固定情報が暗号化された N 個の暗号化固定情報を含み、前記鍵管理方法は、さらに、
N 個の暗号化固定情報を読み出す暗号化固定情報読出ステップと、
N 個の復号鍵セットを用いて、前記読み出した N 個の暗号化固定情報を復号する暗号化固定情報復号ステップとを含み、
前記所定の基準とは、暗号化固定情報を復号して復号文を生成し、生成された復号文に固定値からなる固定情報が含まれることであることを特徴とする請求項 3 8 記載の鍵管理方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、デジタル化された文書、音声、画像、プログラムなどのデジタル著作物を暗号化して伝送媒体や記録媒体を介して伝送する暗号システムに関し、特に、1 台の鍵管理装置が、複数の種類の暗号装置と複数の種類の復号装置とを管理する技術に

関する。

【0002】

【従来の技術】 従来、デジタル化された文書、音声、画像、プログラムなどのデジタル著作物を市場などに流通させる場合には、デジタル著作物が不正に使用されないように、暗号装置により秘密鍵を用いて暗号化されたデジタル著作物を伝送媒体や記録媒体（以下、配布媒体と呼ぶ。）を介して配布し、復号装置により復号鍵を用いて復号している。

【0003】

【発明が解決しようとする課題】 しかしながら、復号鍵が不正に解読されデジタル著作物が不正に使用されたり、配布媒体が不正に複製される場合がある。このため、暗号システムは、復号鍵が不正に解読されにくくしなければならないという第 1 の問題点がある。この第 1 の問題点を解決するためには、異なる暗号鍵を有する暗号装置が複数あるほうがよい。また、暗号装置の保有する鍵の総量は、鍵管理装置の保有する鍵の総量よりも少ないことが望ましい。

【0004】 また、1 つの復号装置の復号鍵が解読された場合に、他の復号装置にもその影響が及び、解読された復号鍵が利用されて、他の復号装置において不正にデジタル著作物が利用されるという第 2 の問題点がある。この第 2 の問題点を解決するためには、異なる復号装置には、異なる復号鍵が割り当てられることが望ましい。このとき、暗号化されたデータがどのような復号装置においても首尾よく復号できるようにするため、暗号装置が全ての異なる復号装置に対応する暗号鍵を備え、データをそれぞれの暗号鍵で暗号化して複数の暗号化データを生成して配布し、復号装置は、配布される複数の暗号化データから、当該復号装置向けの暗号化データを判別して取り出し、これを復号する暗号システムが提案されている。また、復号装置に、複数の鍵を割り当てる暗号システムが提案されている。さらに、配布媒体が不正に複製された疑いがある場合などに、複製に用いられたオリジナルの配布媒体の生産元や流通経路を特定するために、当該オリジナルの配布媒体の生産に用いられた暗号装置を特定する必要があるという第 3 の問題点がある。

【0005】 本発明は、上記に示す第 1、第 2 の問題点を解決するため、異なる暗号鍵を有する暗号装置を複数有し、暗号装置の保有する鍵の総量は、鍵管理装置の保有する鍵の総量よりも少なく、異なる復号装置には異なる復号鍵が複数個割り当てられ、さらに、上記に示す第 3 の問題点を解決するため、配布媒体が不正に複製された疑いがある場合などに、配布媒体がどの種類の暗号装置により生産されたものであるかを識別することのできる暗号システムを提供することを目的とする。

【0006】

【課題を解決するための手段】 上記目的を達成するために、本発明は、1 台の鍵管理装置と、M (M は 2 以上の

整数) 種類の暗号装置と、N (Nは2以上の整数) 種類の復号装置とからなる暗号システムであって、前記鍵管理装置は、復号鍵セットをN個記憶し、暗号鍵セットをM個記憶し、N個の識別番号を記憶し、前記M個の暗号鍵セットをそれぞれ前記M種類の暗号装置に配布し、前記N個の復号鍵セットをそれぞれ前記N種類の復号装置に配布し、前記N個の識別番号をそれぞれ前記N種類の復号装置に配布し、前記暗号鍵セットはN個の暗号鍵からなり、前記復号鍵セットは所定数の復号鍵からなり、前記M種類の暗号装置のそれぞれは、デジタルデータをスクランブルキーを用いて暗号化して暗号化デジタルデータを生成し、前記配布された暗号鍵セットを用いて前記スクランブルキーを暗号化してN個の暗号化スクランブルキーを生成し、前記暗号化デジタルデータと前記N個の暗号化スクランブルキーとを配布媒体に書き込み、前記N種類の復号装置のそれぞれは、前記配布された復号鍵セットに含まれる前記所定数の復号鍵を用いて、前記配布媒体に含まれる前記配布された識別番号により特定される1つの暗号化スクランブルキーを順次復号し、第1の所定の基準により正しく復号されたスクランブルキーを用いて前記配布媒体に含まれる暗号化デジタルデータを復号してデジタルデータを生成し、識別番号は、配布媒体に書き込まれているN個の暗号化スクランブルキーから当該復号装置に対応する1つの暗号化スクランブルキーを識別し、前記鍵管理装置は、さらに、前記配布媒体から1つの暗号化スクランブルキーを読み出す第1暗号文読出手段と、1つの復号鍵セットを読み出す復号鍵セット読出手段と、前記読み出した復号鍵セットに含まれる前記所定数の復号鍵を用いて、前記読み出した暗号化スクランブルキーを順次復号し、前記第1の所定の基準により正しく暗号化スクランブルキーを復号する復号鍵を、前記所定数の復号鍵の中から1つ選択する復号鍵選択手段と、前記配布媒体からN個の暗号化スクランブルキーの読み出しが終了するまで、前記第1暗号文読出手段、前記復号鍵セット読出手段、前記復号鍵選択手段に対して、暗号化スクランブルキーの読み出しと、復号鍵セットの読み出しと、読み出した暗号化スクランブルキーの復号とを繰り返すように制御し、その結果N個の復号鍵のセットが選択される第1繰返制御手段と、前記M個の暗号鍵セットから、前記選択されたN個の復号鍵のセットと一致する1つの暗号鍵セットを検出し、検出された暗号鍵セットにより特定される暗号装置を識別する鍵パターン検出手段とを備えることを特徴とする。

【0007】ここで、前記鍵管理装置は、所定数の復号鍵からなる復号鍵セットをN個記憶している第1復号鍵記憶手段と、前記第1復号鍵記憶手段に記憶されているN個の復号鍵セットのそれぞれから、第1の所定の方法により1つの復号鍵を選択して1つの暗号鍵とし、N個の暗号鍵からなる暗号鍵セットを生成する暗号鍵生成手段と、前記生成された1つの暗号鍵セットを記憶する第

1暗号鍵記憶手段と、M個の暗号鍵セットが生成されるまで、前記暗号鍵生成手段に対して、暗号鍵セットの生成を繰り返すように制御し、その結果、前記第1暗号鍵記憶手段はM個の暗号鍵セットを記憶する第2繰返制御手段と、前記第1暗号鍵記憶手段に記憶されているM個の暗号鍵セットをそれぞれ前記M種類の暗号装置に配布する暗号鍵セット配布手段と、前記第1復号鍵記憶手段に記憶されているN個の復号鍵セットをそれぞれ前記N種類の復号装置に配布する復号鍵セット配布手段と、N個の識別番号をそれぞれ前記N種類の復号装置に配布する識別番号配布手段とを備えるように構成してもよい。

【0008】ここで、前記第1の所定の方法とは、前記第1復号鍵記憶手段に記憶されているN個の復号鍵セットのそれぞれから、ランダムに1個の復号鍵を選択することであるように構成してもよい。

【0009】ここで、前記第1の所定の方法とは、前記第1復号鍵記憶手段に記憶されているN個の復号鍵セットのそれぞれから、一様にランダムに1個の復号鍵を選択することであるように構成してもよい。

【0010】ここで、前記M種類の暗号装置のそれぞれは、前記鍵管理装置から配布された1つの暗号鍵セットを受信し、受信した前記暗号鍵セットを記憶する第2暗号鍵記憶手段と、スクランブルキーを生成するスクランブルキー生成手段と、外部からデジタルデータを受信し、受信したデジタルデータを前記生成されたスクランブルキーを用いて暗号化し、暗号化デジタルデータを生成するデジタルデータ暗号化手段と、前記第2暗号鍵記憶手段に記憶されている暗号鍵セットに含まれるN個の暗号鍵を用いて、第2の所定の方法により、前記スクランブルキーを順次暗号化し、N個の暗号化スクランブルキーを生成する鍵暗号化手段と、前記生成された暗号化デジタルデータと前記生成されたN個の暗号化スクランブルキーとを配布媒体に書き込む媒体書込手段とを備えるように構成してもよい。

【0011】ここで、前記第2の所定の方法とは、前記スクランブルキーと固定値からなる固定情報とを結合し、結合されたスクランブルキーと固定情報とを暗号化することであるように構成してもよい。

【0012】ここで、前記第2の所定の方法とは、前記スクランブルキーを暗号化してN個の暗号化スクランブルキーを生成し、さらに、固定値からなる固定情報を暗号化してN個の暗号化固定情報を生成することであり、前記媒体書込手段は、暗号化デジタルデータとN個の暗号化スクランブルキーとN個の暗号化固定情報とを配布媒体に書き込むように構成してもよい。

【0013】ここで、前記復号鍵選択手段は、前記復号鍵セットから復号鍵を順次読み出す第1復号鍵読出手段と、前記読み出した復号鍵を用いて、前記読み出した暗号化スクランブルキーを復号し、復号文を生成する第1復号文生成手段と、前記第1の所定の基準により、復号

文が正しく復号されているかどうかを検査する第 1 復号文検査手段と、前記復号鍵セットから所定数の復号鍵の読出しが終了するまで、前記第 1 復号鍵読出手段、前記第 1 復号文生成手段、前記第 1 復号文検査手段に対して、復号鍵の読出しと、暗号化スクランブルキーの復号と、復号文の検査とを繰り返し行うように制御する第 3 繰返制御手段と、前記復号文検査手段により正しく復号されたと検査された際に用いられた復号鍵を出力する鍵出力手段とを備えるように構成してもよい。

【0014】ここで、前記第 1 の所定の基準とは、前記復号文に固定値からなる固定情報が含まれることであるように構成してもよい。

【0015】ここで、前記配布媒体は、さらに、前記暗号鍵セットに含まれる N 個の暗号鍵を用いて固定値からなる固定情報が暗号化された N 個の暗号化固定情報を含み、前記鍵管理装置は、さらに、N 個の暗号化固定情報を読み出す暗号化固定情報読出手段と、前記 N 個の復号鍵セットを用いて、前記読み出した N 個の暗号化固定情報をそれぞれ復号する暗号化固定情報復号手段とを含み、前記第 1 の所定の基準とは、暗号化固定情報を復号して復号文を生成し、生成された復号文に固定値からなる固定情報が含まれることであるように構成してもよい。

【0016】ここで、前記 N 種類の復号装置のそれぞれは、前記鍵管理装置から識別番号を受信し、受信した識別番号を記憶する識別番号記憶手段と、前記鍵管理装置から配布された 1 つの復号鍵セットを受信し、受信した前記復号鍵セットを記憶する第 2 復号鍵記憶手段と、前記配布媒体から前記受信した識別番号により識別される 1 つの暗号化スクランブルキーを読み出す第 2 暗号文読出手段と、前記配布媒体から暗号化デジタルデータを読み出すデジタルデータ読出手段と、前記第 2 復号鍵記憶手段から前記復号鍵セットに含まれる復号鍵を順次読み出す第 2 復号鍵読出手段と、前記読み出した復号鍵を用いて、前記読み出した暗号化スクランブルキーを復号し、復号文を生成する第 2 復号文生成手段と、前記第 1 の所定の基準により、復号文が正しく復号されているかどうかを検査し、正しく復号された場合に前記復号文をスクランブルキーとする第 2 復号文検査手段と、復号鍵セットから所定数の復号鍵の読出しが終了するまで、前記第 2 復号鍵読出手段、前記第 2 復号文生成手段、前記第 2 復号文検査手段に対して、復号鍵の読出しと、暗号化スクランブルキーの復号と、復号文の検査とを繰り返し行うように制御する第 4 繰返制御手段と、前記復号文検査手段により正しく復号されたと検査されたスクランブルキーを用いて、前記読み出した暗号化デジタルデータを復号し、デジタルデータを生成するデジタルデータ復号手段とを備えるように構成してもよい。

【0017】ここで、前記第 1 の所定の基準とは、前記復号文に固定値からなる固定情報が含まれることである

ように構成してもよい。

【0018】ここで、前記配布媒体は、さらに、前記暗号鍵セットに含まれる N 個の暗号鍵を用いて固定値からなる固定情報が暗号化された N 個の暗号化固定情報を含み、前記復号装置は、さらに、前記識別番号により識別される 1 つの暗号化固定情報を読み出す暗号化固定情報読出手段と、前記復号鍵セットに含まれる所定数の復号鍵を用いて、前記読み出した暗号化固定情報を復号する暗号化固定情報復号手段とを備え、前記第 1 の所定の基準とは、暗号化固定情報を復号して復号文を生成し、生成された復号文に固定値からなる固定情報が含まれることであるように構成してもよい。

【0019】

【発明の実施の形態】本発明に係る 1 つの実施の形態としての暗号システム 10 について説明する。

1. 暗号システム 10 の構成

本発明に係る 1 つの実施の形態としての暗号システム 10 の構成を示すブロック図を図 1 に示す。暗号システム 10 は、この図に示すように、1 つの鍵管理装置 100、M 種類の暗号装置 200、201、・・・、202、N 種類の復号装置 300、301、・・・、302 から構成される。ここで、M 及び N は、2 以上の整数である。

【0020】鍵管理装置 100 は、M 種類の暗号鍵セット記録媒体 21 を生成し、M 種類の暗号鍵セット記録媒体 21 は、それぞれ M 種類の暗号装置 200、201、・・・、202 に配布される。また、鍵管理装置 100 は、N 種類の復号鍵セット記録媒体 22 を生成し、N 種類の復号鍵セット記録媒体 22 は、それぞれ N 種類の復号装置 300、301、・・・、302 に配布される。M 種類の暗号装置 200、201、・・・、202 のそれぞれは、デジタル著作物記録媒体 31 に記録されているデジタル著作物を暗号化し、暗号化したデジタル著作物を M 種類の配布媒体 40、41、・・・、42 に書き込む。N 種類の復号装置 300、301、・・・、302 のそれぞれは、M 種類の配布媒体 40、41、・・・、42 のいずれかから暗号化されたデジタル著作物を読み出し、復号する。また、鍵管理装置 100 は、配布媒体 50 を生産した暗号装置の種類を特定する。以下に、上記の各装置の構成について詳細に説明する。

【0021】1. 1 鍵管理装置 100 の構成

鍵管理装置 100 は、図 2 に示すように、復号鍵セット配布部 111、復号鍵テーブル 112、暗号鍵生成部 113、暗号鍵テーブル 114、暗号鍵生成制御部 115、暗号鍵セット配布部 116、識別番号配布部 121、識別番号記憶部 122、復号選択制御部 131、復号鍵セット読出部 132、暗号文読出部 133、復号選択部 134、鍵パターン検出部 135、暗号装置管理処理部 136 から構成され、復号選択部 134 は、図 3 に示すように、復号鍵読出部 141、復号制御部 142、

復号文生成部 143、復号文検査部 144、鍵出力部 145 から構成される。鍵管理装置 100 は、2つの機能を有する。第 1 の機能は、暗号鍵、復号鍵、識別番号の生成と配布である。第 2 の機能は、配布媒体を生産した暗号装置の種類の特定である。

【0022】 1. 1. 1 復号鍵テーブル 112

復号鍵テーブル 112 は、図 4 に示すように、あらかじめ N 個の復号鍵セット 400、401、・・・、402 を有し、N 個の復号鍵セット 400、401、・・・、402 のそれぞれは、R 個の鍵を含む。これらの鍵は、暗号文を復号する際に用いられるものである。ここで、R は 2 以上の整数である。前記復号鍵の長さは、それぞれ 128 ビットである。N 個の復号鍵セット 400、401、・・・、402 は、それぞれ 1、2、・・・、N からなる番号で識別される。また、N 個の復号鍵セット 400、401、・・・、402 のそれぞれに含まれる R 個の鍵は、それぞれ 1、2、・・・、r からなる番号で識別される。ここで、i 番目の復号鍵セットに含まれる j 番目の鍵を K_{ij} と表す。N 個の復号鍵セットは、それぞれ N 種類の復号装置 300、301、・・・、302 に割り当てられる。復号鍵テーブル 112 の一例を図 5 に示す。図 5 に示す復号鍵テーブル 510 は、5 個の復号鍵セット 500、501、502、503、504 を有しており、5 個の復号鍵セット 500、501、502、503、504 のそれぞれは、2 個の鍵を含む。復号鍵セット 500、501、502、503、504 は、それぞれ 5 種類の復号装置 D_1 、 D_2 、 D_3 、 D_4 、 D_5 に割り当てられる。

【0023】 1. 1. 2 暗号鍵生成制御部 115

暗号鍵生成制御部 115 は、暗号鍵生成部 113 に対して、M 個の暗号鍵セット 420、421、・・・、422 を順次生成するように制御する。M 個の暗号鍵セット 420、421、・・・、422 は、それぞれ N 個の鍵を含む。具体的には、暗号鍵生成制御部 115 は、生成された暗号鍵セットの番号を 1 から M まで、1 ずつ順に加算して得られる値を暗号鍵生成部 113 へ出力する。M 個の暗号鍵セット 420、421、・・・、422 は、それぞれ 1、2、・・・、M からなる番号で識別される。また、M 個の暗号鍵セット 420、421、・・・、422 のそれぞれに含まれる N 個の鍵は、それぞれ 1、2、・・・、N からなる番号で識別される。

【0024】 1. 1. 3 暗号鍵生成部 113

暗号鍵生成部 113 は、暗号鍵生成制御部 115 の制御のもとに、暗号鍵生成制御部 115 から番号 1 を受け取ると、1 番目の暗号鍵セット 420 を、次に示すようにして生成する。暗号鍵生成部 113 は、復号鍵テーブル 112 を構成する 1 番目の復号鍵セット 400 に含まれる R 個の鍵から、1 個の鍵をランダムに選択し、選択した 1 個の鍵を 1 番目の鍵として暗号鍵テーブル 114 の 1 番目の暗号鍵セット 420 に書き込む。次に、暗号鍵

生成部 113 は、復号鍵テーブル 112 を構成する 2 番目の復号鍵セット 401 に含まれる R 個の鍵から、1 個の鍵をランダムに選択し、選択した 1 個の鍵を 2 番目の鍵として暗号鍵テーブル 114 の 1 番目の暗号鍵セット 420 に書き込む。暗号鍵生成部 113 は、以下同様にして、3 番目以降の復号鍵セットからランダムに各 1 個の鍵を選択し、3 番目以降の鍵として暗号鍵セット 420 に書き込むことを繰り返す。こうして、暗号鍵生成部 113 は、N 個の鍵を含む暗号鍵セット 420 を、暗号鍵テーブル 114 内に生成する。暗号鍵生成部 113 は、同様にして、暗号鍵生成制御部 115 の制御のもとに、暗号鍵生成制御部 115 から番号 2 から番号 M を受け取ると、2 番目から M 番目までの暗号鍵セットを生成し、暗号鍵テーブル 114 に書き込む。

【0025】 1. 1. 4 暗号鍵テーブル 114

暗号鍵テーブル 114 は、図 4 に示すように、M 個の暗号鍵セット 420、421、・・・、422 を有し、M 個の暗号鍵セット 420、421、・・・、422 のそれぞれは、N 個の鍵を含む。これらの鍵は、平文を暗号化する際に用いられるものである。前記暗号鍵の長さは、それぞれ 128 ビットである。M 個の暗号鍵セットは、それぞれ M 種類の暗号装置 200、201、・・・、202 に割り当てられる。暗号鍵テーブル 114 の一例を図 6 に示す。図 6 に示す暗号鍵テーブル 610 は、4 個の暗号鍵セット 600、601、602、603 を有しており、4 個の暗号鍵セット 600、601、602、603 は、それぞれ 5 個の鍵を含む。暗号鍵セット 600、601、602、603 は、それぞれ 4 種類の暗号装置 E_1 、 E_2 、 E_3 、 E_4 に割り当てられる。

【0026】 1. 1. 5 復号鍵セット配布部 111

復号鍵セット配布部 111 は、復号鍵テーブル 112 から 1 番目の復号鍵セット 400 を読み出し、読み出した 1 番目の復号鍵セット 400 を 1 番目の復号鍵セット記録媒体に書き込む。次に、復号鍵セット配布部 111 は、復号鍵テーブル 112 から 2 番目の復号鍵セット 401 を読み出し、読み出した 2 番目の復号鍵セット 401 を 2 番目の復号鍵セット記録媒体に書き込む。復号鍵セット配布部 111 は、同様にして、3 番目から N 番目までの復号鍵セットの読み出しと 3 番目から N 番目までの復号鍵セット記録媒体へ書き込むとを繰り返す。こうして、復号鍵セット配布部 111 は、復号鍵テーブル 112 の N 個の復号鍵セットのそれぞれを N 個の復号鍵セット記録媒体へ書き込む。

【0027】 1. 1. 6 暗号鍵セット配布部 116

暗号鍵セット配布部 116 は、暗号鍵テーブル 114 から 1 番目の暗号鍵セット 420 を読み出し、読み出した 1 番目の暗号鍵セット 420 を 1 番目の暗号鍵セット記録媒体に書き込む。次に、暗号鍵セット配布部 116 は、暗号鍵テーブル 114 から 2 番目の暗号鍵セット 4

21を読み出し、読み出した2番目の暗号鍵セット421を2番目の暗号鍵セット記録媒体に書き込む。暗号鍵セット配布部116は、同様にして、3番目からM番目までの暗号鍵セットの読み出しと3番目からM番目までの暗号鍵セット記録媒体への書き込みとを繰り返す。こうして、暗号鍵セット配布部116は、暗号鍵テーブル114のM個の暗号鍵セットのそれぞれをM個の暗号鍵セット記録媒体へ書き込む。

【0028】1. 1. 7 識別番号記憶部122

識別番号記憶部122は、N個の識別番号を記憶している。N個の識別番号は、N種類の復号装置300、301、・・・、302にそれぞれ対応している。識別番号は、各復号装置が配布媒体に書き込まれている暗号化デジタル著作物を復号する際に、配布媒体に書き込まれているN個の暗号化スクランブルキーの中から当該復号装置に対応した1つの暗号化スクランブルキーを識別するために用いられる。

【0029】1. 1. 8 識別番号配布部121

識別番号配布部121は、N個の復号鍵セット記録媒体毎に、各復号装置に対応する識別番号を、識別番号記憶部122より、読み出し、読み出した識別番号を対応する復号鍵セット記録媒体に書き込む。

【0030】1. 1. 9 復号選択制御部131

復号選択制御部131は、配布媒体50からN個の暗号化スクランブルキーの読み出しが終了するまで、暗号文読出部133と、復号鍵セット読出部132と、復号選択部134とに対して、暗号化スクランブルキーの読み出しと、復号鍵セットの読み出しと、読み出した暗号化スクランブルキーの復号とをN回繰り返し行うように、制御する。なお、暗号化スクランブルキーについては、後述する。具体的には、復号選択制御部131は、番号1の暗号化スクランブルキーを読み出すように、暗号文読出部133に対して制御し、次に、番号1の復号鍵セットを読み出すように、復号鍵セット読出部132に対して制御し、次に、番号1の復号鍵セットに含まれるR個の鍵を用いて、前記読み出した番号1の暗号化スクランブルキーを復号し、第1の所定の基準により、正しく暗号化スクランブルキーを復号する鍵を、前記R個の鍵の中から1つ選択するように、復号選択部134に対して制御する。続けて、復号選択制御部131は、番号2から番号Nについて、上記の制御を繰り返す。上記の繰り返しが終了すると、N個の復号されたスクランブルキーを含む復号文が復号される際に用いられたN個の鍵のセットが選択される。

【0031】1. 1. 10 暗号文読出部133

暗号文読出部133は、復号選択制御部131の制御の元に、暗号化スクランブルキーの番号の指定を受けて、配布媒体50から、前記指定された番号により特定される一つの暗号化スクランブルキーを読み出す。

【0032】1. 1. 11 復号鍵セット読出部132

復号鍵セット読出部132は、復号選択制御部131の制御の元に、復号鍵セットの番号の指定を受けて、復号鍵テーブル112から、前記指定された番号により特定される一つの復号鍵セットを読み出す。

【0033】1. 1. 12 復号選択部134

復号選択部134は、復号選択制御部131の制御の元に、復号鍵セット読出部132により読み出された1つの復号鍵セットに含まれるR個の鍵を用いて、暗号文読出部133により読み出された暗号化スクランブルキーを復号し、第1の所定の基準により、正しく暗号化スクランブルキーを復号する鍵を、前記R個の鍵の中から1つ選択する。復号選択部134を構成する復号鍵読出部141、復号制御部142、復号文生成部143、復号文検査部144、鍵出力部145について、以下に説明する。

【0034】(1) 復号鍵読出部141

復号鍵読出部141は、復号制御部142の制御の元に、復号鍵セット読出部132により読み出された復号鍵セットから、復号制御部142から読み出す鍵の番号の指定を受けて、指定された番号により特定される1つの鍵を読み出す。

【0035】(2) 復号文生成部143

復号文生成部143は、復号制御部142の制御の元に、復号鍵読出部141により読み出された鍵を用いて、前記暗号文読出部133により読み出された暗号化スクランブルキーを含む暗号文を復号し、スクランブルキーを含む復号文を生成する。なお、復号文生成部143の構成は、後述する復号文生成部306と同様であるので、説明を省略する。

【0036】(3) 復号文検査部144

復号文検査部144は、復号制御部142の制御の元に、復号文生成部143により生成されたスクランブルキーを含む復号文が、第1の所定の基準により、正しく復号されているかどうかを検査する。ここで、第1の所定の基準とは、図7に示すように、スクランブルキーを含む復号文の前半の64ビットに固定値からなる固定情報が含まれることである。前記固定値は、64ビットの連続する0である。スクランブルキーを含む復号文の後半の64ビットはスクランブルキーである。すなわち、復号文検査部144は、生成されたスクランブルキーを含む復号文の前半の64ビットが連続する0である場合には、復号鍵読出部141により読み出され、復号に用いられた鍵が正しく、正しくスクランブルキーが復号されたものとみなす。生成されたスクランブルキーを含む復号文の前半の64ビットが連続する0以外である場合には、復号鍵読出部141により読み出され、復号に用いられた鍵が誤っていたものとみなす。

【0037】(4) 復号制御部142

復号制御部142は、復号鍵セット読出部132により読み出された復号鍵セットからR個の鍵の読出しが終了

するまで、復号鍵読出部141、復号文生成部143、復号文検査部144に対して、鍵の読出しと、暗号化スクランブルキーの復号と、復号されたスクランブルキーの検査とをR回繰り返すように制御する。具体的には、復号制御部142は、復号鍵セット読出部132により読み出された復号鍵セットから、番号1の鍵を読み出すように、復号鍵読出部141に対して制御し、次に、番号1の鍵を用いて、暗号文読出部133により読み出された暗号化スクランブルキーを復号するように、復号文生成部143に対して制御し、次に、復号文生成部143により生成されたスクランブルキーが正しく復号されているかどうかを検査するように、復号文検査部144を制御する。復号選択制御部131は、番号2から番号Rについて、上記の制御を繰り返す。上記の繰り返しが終了すると、復号鍵読出部141により読み出され、正しく復号された1個のスクランブルキーが復号される際に用いられた1個の鍵が選択される。

【0038】(5) 鍵出力部145

鍵出力部145は、前記復号文検査部144により正しく復号されたと検査された1個のスクランブルキーを復号する際に用いられた1個の鍵を、鍵パターン検出部135へ出力する。

【0039】1. 1. 13 鍵パターン検出部135

鍵パターン検出部135は、暗号鍵テーブル114に記憶されているM個の暗号鍵セット420、421、・・・、422から、復号選択制御部131によって前記選択されたN個の鍵のセットと一致する1つの暗号鍵セットを検出し、検出された暗号鍵セットの番号を暗号装置管理処理部136へ出力する。この番号により特定される暗号装置により、配布媒体50が生産されたものと分かる。

【0040】1. 1. 14 暗号装置管理処理部136

暗号装置管理処理部136は、鍵パターン検出部135より、検出された暗号鍵セットの番号を受け取る。暗号装置管理処理部136は、M種類の暗号装置毎に、暗号装置の番号と、暗号装置の名称と、暗号装置の製造メーカーとを記憶している。暗号装置管理処理部136は、前記受け取った番号を基にして、前記記憶内容より、暗号装置の名称と、暗号装置の製造メーカーとを検索し、検索された暗号装置の名称と、暗号装置の製造メーカーとを表示する。

【0041】1. 2 鍵管理装置100の動作

ここでは、鍵管理装置100の鍵生成と鍵の配布の動作と、鍵管理装置100の暗号装置を特定する動作について説明する。

【0042】1. 2. 1 鍵管理装置100の鍵生成と鍵の配布の動作

鍵管理装置100の鍵生成と鍵の配布の動作について、図8に示すフローチャートを用いて説明する。暗号鍵生成制御部115は、iの値を1からMまで1ずつ増加さ

せて変化させて、暗号鍵生成部113に対して暗号鍵セットの生成制御を繰り返す(ステップS801～ステップS806)。ここで、iは、正の整数の値をとるカウンタである。暗号鍵生成部113は、jの値を1からNまで1ずつ増加させて変化させて(ステップS802～ステップS805)、復号鍵セットに含まれるR個の鍵から、1個の鍵をランダムに選択し、(ステップS803)、選択した1個の鍵をj番目の鍵として暗号鍵テーブル114のi番目の暗号鍵セットに書き込む(ステップS804)動作をN回繰り返す。ここで、jは、正の整数の値をとるカウンタである。次に、暗号鍵セット配布部116は、暗号鍵テーブル114のM個の暗号鍵セットのそれぞれをM個の暗号鍵セット記録媒体へ書き込み(ステップS807～ステップS810)、復号鍵セット配布部111は、復号鍵テーブル112のN個の復号鍵セット及び識別番号記憶部のN個の識別番号のそれぞれをN個の復号鍵セット記録媒体へ書き込む(ステップS811～ステップS813)。

【0043】1. 2. 2 鍵管理装置100の暗号装置を特定する動作

鍵管理装置100の暗号装置を特定する動作について、図9に示すフローチャートを用いて説明する。復号選択制御部131は、nを1からNまで、1ずつ加算することにより、配布媒体50からN個の暗号化スクランブルキーの読み出しが終了するまで、暗号文読出部133と、復号鍵セット読出部132と、復号選択部134とに対して、暗号化スクランブルキーの読み出し(ステップS902)と、復号鍵セットの読み出し(ステップS903)と、読み出した暗号化スクランブルキーの復号と鍵の選択(ステップS904)とをN回繰り返すように、制御する(ステップS901～ステップS910)。ここで、nは、正の整数の値をとるカウンタである。上記の繰り返しが終了すると、N個の復号されたスクランブルキーを含む復号文が復号される際に用いられたN個の鍵のセットが選択される。ここで、暗号化スクランブルキーの復号(ステップS904)では、復号制御部142は、rを1からRまで、1ずつ加算することにより、復号鍵セット読出部132により読み出された復号鍵セットからR個の第1鍵の読出しが終了するまで、復号鍵読出部141、復号文生成部143、復号文検査部144に対して、鍵の読出し(ステップS906)と、暗号化スクランブルキーの復号(ステップS907)と、復号されたスクランブルキーの検査(ステップS908)とをR回繰り返すように制御する。ここで、rは、正の整数の値をとるカウンタである。

【0044】次に、鍵パターン検出部135は、mを1からMまで、1ずつ加算することにより、暗号鍵テーブル114に記憶されているM個の暗号鍵セット420、421、・・・、422から、前記選択されたN個の鍵のセットと一致する1つの暗号鍵セットを検出し(ステ

ップS911～ステップS913)、検出された暗号鍵セットの番号を暗号装置管理処理部136へ出力し、暗号装置管理処理部136は、前記受け取った番号を基にして、暗号装置の名称と、暗号装置の製造メーカーとを表示する(ステップS914)。ここで、mは、正の整数の値をとるカウンタである。

【0045】1. 3 暗号装置200の構成

ここでは、暗号装置200の構成について説明する。なお、暗号装置201、・・・、202については同様の構成であるので説明を省略する。暗号装置200は、図10に示すように、暗号鍵記憶部205、デジタルデータ暗号化部202、スクランブルキー生成部203、鍵暗号化部204から構成される。

【0046】1. 3. 1 暗号鍵記憶部205

暗号鍵記憶部205は、配布された暗号鍵セット記録媒体21から、N個の鍵を含む1つの暗号鍵セットを読み出し、読み出した1つの暗号鍵セットを記憶する。ここで、N個の鍵はそれぞれ128ビットの長さである。

【0047】1. 3. 2 スクランブルキー生成部203

スクランブルキー生成部203は、乱数を用いて、64ビットのスクランブルキーを生成し、64ビットの連続する0と前記生成された64ビットのスクランブルキーとを結合し、結合された64ビットの連続する0と前記生成された64ビットのスクランブルキーとを鍵暗号化部204へ出力する。また、スクランブルキー生成部203は、前記生成された64ビットのスクランブルキーをデジタルデータ暗号化部202へ出力する。

【0048】1. 3. 3 鍵暗号化部204

鍵暗号化部204は、図11に示すように、分解部211、DES暗号化部212、213、分解部214、結合部215から構成される。

【0049】(1) 分解部211

分解部211は、スクランブルキー生成部203から出力された、結合された64ビットの連続する0と64ビットのスクランブルキーとを、64ビットの連続する0と64ビットのスクランブルキーとに分解し、64ビットの連続する0をDES暗号化部212へ出力し、64ビットのスクランブルキーをDES暗号化部213へ出力する。

【0050】(2) 分解部214

分解部214は、暗号鍵記憶部205から、N個の鍵を、N回繰り返して順次読み出し、読み出した各鍵を前半の64ビットと、後半の64ビットに分解し、前半の64ビットをDES暗号化部212へ出力し、後半の64ビットをDES暗号化部213へ出力する。

【0051】(3) DES暗号化部212

DES暗号化部212は、分解部214から出力された64ビットの鍵を用いて、データ暗号化規格(DES、Data Encryption Standard)

により規格されるDES暗号化アルゴリズムにより、分解部211から出力された64ビットの連続する0を暗号化して64ビットの暗号文を生成し、生成された64ビットの暗号文を結合部215へ出力する。DESについては、公知であるので、説明を省略する。

【0052】(4) DES暗号化部213

DES暗号化部213は、分解部214から出力された64ビットの鍵を用いて、DES暗号化アルゴリズムにより、分解部211から出力された64ビットのスクランブルキーを暗号化し、64ビットの暗号文を生成し、生成された64ビットの暗号文を結合部215へ出力する。

【0053】(5) 結合部215

結合部215は、DES暗号化部212から出力された64ビットの暗号文と、DES暗号化部213から出力された64ビットの暗号文とをこの順で結合し、結合されて生成された128ビットの暗号文を配布媒体40に書き込む。このようにして、N個の暗号文が配布媒体40に書き込まれる。ここで、前記128ビットの暗号文を暗号化スクランブルキーと呼ぶ。

【0054】1. 3. 4 デジタルデータ暗号化部202

デジタルデータ暗号化部202は、デジタル著作物記録媒体31に記録されているデジタル著作物を読み出し、スクランブルキー生成部203から出力された64ビットのスクランブルキーを用いて、DES暗号化アルゴリズムにより、前記読み出したデジタル著作物を暗号化して、暗号化デジタル著作物を生成し、生成した暗号化デジタル著作物を配布媒体40に書き込む。

【0055】デジタルデータ暗号化部202の動作について、図12に示すフローチャートを用いて説明する。

デジタルデータ暗号化部202は、スクランブルキー生成部203から出力された64ビットのスクランブルキーを受け取り(ステップS1201)、デジタル著作物記録媒体31に記録されているデジタル著作物から64ビット分のデジタルデータを読み出し(ステップS1202)、デジタルデータの読み出しが終了していれば(ステップS1203)、処理を終了し、デジタルデータの読み出しが終了していなければ(ステップS1203)、前記64ビットのスクランブルキーを用いて、DES暗号化アルゴリズムにより、読み出した64ビット分のデジタルデータを暗号化して、64ビット分の暗号化デジタルデータを生成し(ステップS1204)、生成した暗号化デジタルデータを配布媒体40に書き込む(ステップS1205)。次に、再度ステップS1202に制御を戻し、デジタルデータの読み出しが終了するまで、デジタルデータの読み出しとデジタルデータの暗号化と暗号化デジタルデータの配布媒体への書き込みを繰り返す。

【0056】1. 4 暗号装置200の動作

ここでは、暗号装置 200 の動作について、図 13 に示すフローチャートを用いて説明する。なお、暗号装置 201、・・・、202 についても同様であるので、説明は省略する。暗号鍵記憶部 205 は、配布された暗号鍵セット記録媒体 21 から、N 個の鍵を含む 1 つの暗号鍵セットを読み出し、読み出した 1 つの暗号鍵セット 420 を記憶する (ステップ S1311)。スクランブルキー生成部 203 は、乱数を用いて、64 ビットのスクランブルキーを生成し、64 ビットの連続する 0 と前記生成された 64 ビットのスクランブルキーとを結合し、結合された 64 ビットの連続する 0 と前記生成された 64 ビットのスクランブルキーとを鍵暗号化部 204 へ出力し、前記生成された 64 ビットのスクランブルキーをデジタルデータ暗号化部 202 へ出力する (ステップ S1312)。

【0057】分解部 211 は、スクランブルキー生成部 203 から出力された、結合された 64 ビットの連続する 0 と 64 ビットのスクランブルキーとを、64 ビットの連続する 0 と 64 ビットのスクランブルキーとに分解し、64 ビットの連続する 0 を DES 暗号化部 212 へ出力し、64 ビットのスクランブルキーを DES 暗号化部 213 へ出力し、分解部 214 は、暗号鍵記憶部 205 から、N 個の鍵を、N 回繰り返して順次読み出し、読み出した各鍵を前半の 64 ビットと、後半の 64 ビットに分解し、前半の 64 ビットを DES 暗号化部 212 へ出力し、後半の 64 ビットを DES 暗号化部 213 へ出力し、DES 暗号化部 212 は、分解部 214 から出力された 64 ビットの鍵を用いて、データ暗号化規格 (DES, Data Encryption Standard) により規格される DES 暗号化アルゴリズムにより、分解部 211 から出力された 64 ビットの連続する 0 を暗号化して 64 ビットの暗号文を生成し、生成された 64 ビットの暗号文を結合部 215 へ出力し、DES 暗号化部 213 は、分解部 214 から出力された 64 ビットの鍵を用いて、DES 暗号化アルゴリズムにより、分解部 211 から出力された 64 ビットのスクランブルキーを暗号化し、64 ビットの暗号文を生成し、生成された 64 ビットの暗号文を結合部 215 へ出力し、結合部 215 は、DES 暗号化部 212 から出力された 64 ビットの暗号文と、DES 暗号化部 213 から出力された 64 ビットの暗号文とをこの順で結合し、結合されて生成された 128 ビットの暗号文を配布媒体 40 に書き込む。このようにして、N 個の暗号化スクランブルキーが配布媒体 40 に書き込まれる (ステップ S1313)。

【0058】デジタルデータ暗号化部 202 は、デジタル著作物記録媒体 31 に記録されているデジタル著作物を読み出し、スクランブルキー生成部 203 から出力された 64 ビットのスクランブルキーを用いて、DES 暗号化アルゴリズムにより、前記読み出したデジタル著作

物を暗号化して、暗号化デジタル著作物を生成し、生成した暗号化デジタル著作物を配布媒体 40 に書き込む (ステップ S1314)。このようにして、図 14 に示すように、配布媒体 40 には、N 個の暗号化スクランブルキー 1301、1302、・・・、1303 と暗号化デジタル著作物 1304 とが書き込まれる。

【0059】1. 5 復号装置 300 の構成

ここでは、復号装置 300 の構成について説明する。なお、復号装置 301、・・・、302 については同様の構成であるので説明を省略する。復号装置 300 は、図 15 に示すように、識別番号記憶部 311、復号鍵記憶部 312、復号鍵読出部 303、復号検査制御部 304、暗号文読出部 305、復号文生成部 306、復号文検査部 307、デジタルデータ読出部 308、デジタルデータ復号部 309、表示部 310 から構成される。

【0060】1. 5. 1 識別番号記憶部 311

識別番号記憶部 311 は、復号鍵セット記録媒体 22 から、識別番号を読み出し、読み出した識別番号を記憶する。

【0061】1. 5. 2 復号鍵記憶部 312

復号鍵記憶部 312 は、復号鍵セット記録媒体 22 から、R 個の鍵を含む復号鍵セットを読み出し、読み出した復号鍵セットを記憶する。

【0062】1. 5. 3 暗号文読出部 305

暗号文読出部 305 は、識別番号記憶部 311 に記憶されている識別番号を読み出し、読み出した識別番号により識別される 1 つの暗号化スクランブルキーを配布媒体から読み出し、読み出した 1 つの暗号化スクランブルキーを復号文生成部 306 へ出力する。

【0063】1. 5. 4 復号検査制御部 304

復号検査制御部 304 は、復号鍵セットから R 個の鍵の読み出しが終了するまで、復号鍵読出部 303、復号文生成部 306、復号文検査部 307 に対して、1 つの鍵の読み出しと、暗号化スクランブルキーの復号と、暗号化スクランブルキーを復号して得られた復号文の検査とを R 回繰り返すように制御する。具体的には、復号検査制御部 304 は、復号鍵セットから番号 1 の鍵を読み出すように、復号鍵読出部 303 に対して制御する。次に、読み出された番号 1 の鍵を用いて、暗号化スクランブルキーを復号して復号文を生成するように、復号文生成部 306 に対して制御する。さらに、生成された復号文を、前記第 1 の所定の基準により、正しく復号されているかどうかを検査するように、復号文検査部 307 に対して制御する。続けて、復号検査制御部 304 は、番号 2 から番号 R の鍵について、上記の制御を繰り返す。上記の繰り返しが終了すると、R 個の鍵から、暗号化スクランブルキーを正しく復号する 1 つの鍵が選択される。

【0064】1. 5. 5 復号鍵読出部 303

復号鍵読出部 303 は、復号検査制御部 304 の制御の

元で、復号鍵記憶部 302 に記憶されている復号鍵セットの中から、復号検査制御部 304 により指定される番号の 1 つの鍵を読み出し、読み出した 1 つの鍵を復号文生成部 306 へ出力する。

【0065】 1. 5. 6 復号文生成部 306

復号文生成部 306 は、図 16 に示すように、分解部 321、DES 復号部 322、DES 復号部 323、分解部 324、結合部 325 から構成され、復号検査制御部 304 の制御の元に動作する。

【0066】 (1) 分解部 321

分解部 321 は、暗号文読出部 305 から出力される暗号化スクランブルキーを受け取る。この暗号化スクランブルキーは、128 ビットの長さを有する。分解部 321 は、受け取った暗号化スクランブルキーを前半の 64 ビットのデータと後半の 64 ビットとのデータに分解し、前半の 64 ビットのデータを DES 復号部 322 へ出力し、後半の 64 ビットのデータを DES 復号部 323 へ出力する。

【0067】 (2) 分解部 324

分解部 324 は、復号鍵読出部 303 から出力される 1 つの鍵を受け取る。この 1 つの鍵は、128 ビットの長さを有する。分解部 324 は、受け取った 1 つの鍵を前半の 64 ビットのデータと後半の 64 ビットとのデータに分解し、前半の 64 ビットのデータを DES 復号部 322 へ出力し、後半の 64 ビットのデータを DES 復号部 323 へ出力する。

【0068】 (3) DES 復号部 322

DES 復号部 322 は、分解部 324 から出力された 64 ビットの鍵を用いて、データ暗号化規格 (DES、Data Encryption Standard) により規格される DES 復号アルゴリズムにより、分解部 321 から出力された 64 ビットのデータを暗号化して 64 ビットの復号文を生成し、生成された 64 ビットの復号文を結合部 325 へ出力する。

【0069】 (4) DES 復号部 323

DES 復号部 323 は、分解部 324 から出力された 64 ビットの鍵を用いて、DES 復号アルゴリズムにより、分解部 321 から出力された前半 64 ビットのデータを復号して 64 ビットの復号文を生成し、生成された 64 ビットの復号文を結合部 325 へ出力する。

【0070】 (5) 結合部 325

結合部 325 は、DES 復号部 322 から出力された後半 64 ビットの復号文と、DES 復号部 323 から出力された 64 ビットの復号文とをこの順で結合し、結合されて生成された 128 ビットの復号文を復号文検査部 307 へ出力する。

【0071】 1. 5. 7 復号文検査部 307

復号文検査部 307 は、復号検査制御部 304 の制御の元に、復号文生成部 306 により生成されたスクランブルキーを含む復号文が、前記第 1 の所定の基準により、

正しく復号されているかどうかを検査する。すなわち、復号文検査部 307 は、生成されたスクランブルキーを含む復号文の前半の 64 ビットが連続する 0 である場合には、復号鍵読出部 303 により読み出され、復号に用いられた鍵が正しく、正しくスクランブルキーが復号されたものとみなす。生成されたスクランブルキーを含む復号文の前半の 64 ビットが連続する 0 以外である場合には、復号鍵読出部 303 により読み出され、復号に用いられた鍵が誤っていたものとみなす。復号文検査部 307 は、正しく復号されたとする場合に、生成されたスクランブルキーを含む復号文の後半の 64 ビットからなるスクランブルキーをデジタルデータ復号部 309 へ出力する。

【0072】 1. 5. 8 デジタルデータ読出部 308
デジタルデータ読出部 308 は、配布媒体に記憶されている暗号化デジタル著作物を読み出し、読み出した暗号化デジタル著作物をデジタルデータ復号部 309 へ出力する。

【0073】 1. 5. 9 デジタルデータ復号部 309
デジタルデータ復号部 309 は、復号文検査部 307 から受け取ったスクランブルキーを用いて、DES 復号アルゴリズムにより、デジタルデータ読出部 308 により読み出された暗号化デジタル著作物を復号して、デジタル著作物を生成し、生成されたデジタル著作物を表示部 310 へ出力する。デジタルデータ復号部 309 の動作について、図 17 に示すフローチャートを用いて説明する。

【0074】 デジタルデータ復号部 309 は、復号文検査部 307 から出力された 64 ビットのスクランブルキーを受け取り (ステップ S1701)、デジタルデータ読出部 308 により読み出された暗号化デジタル著作物から 64 ビット分の暗号化デジタルデータを読み出し (ステップ S1702)、暗号化デジタルデータの読み出しが終了していれば (ステップ S1703)、処理を終了し、暗号化デジタルデータの読み出しが終了していなければ (ステップ S1703)、前記 64 ビットのスクランブルキーを用いて、DES 復号アルゴリズムにより、読み出した 64 ビット分の暗号化デジタルデータを復号して、64 ビット分のデジタルデータを生成し (ステップ S1704)、生成したデジタルデータを表示部 310 へ出力する (ステップ S1705)。次に、再度ステップ S1702 に制御を戻し、暗号化デジタルデータの読み出しが終了するまで、暗号化デジタルデータの読み出しと暗号化デジタルデータの復号化とデジタルデータの表示部 310 への出力を繰り返す。

【0075】 1. 5. 10 表示部 310

表示部 310 は、デジタルデータ復号部 309 から出力される 64 ビットの復号されたデジタルデータを繰り返し受け取り、順次表示する。

【0076】 1. 6 復号装置 300 の動作

ここでは、復号装置300の動作について、図18に示すフローチャートを用いて説明する。なお、復号装置301、・・・、302についても、同様であるので、説明を省略する。識別番号記憶部311は、復号鍵セット記録媒体22から、識別番号を読み出し、読み出した識別番号を記憶する(ステップS1801)。復号鍵記憶部302は、復号鍵セット記録媒体22から、R個の鍵を含む復号鍵セットを読み出し、読み出した復号鍵セットを記憶する(ステップS1802)。

【0077】暗号文読出部305は、識別番号記憶部311に記憶されている識別番号を読み出し、読み出した識別番号により識別される1つの暗号化スクランブルキーを配布媒体から読み出し、読み出した1つの暗号化スクランブルキーを復号文生成部306へ出力する(ステップS1803)。復号検査制御部304は、rを1からRまで、1つずつ加算することにより、復号鍵セットからR個の鍵の読み出しが終了するまで、復号鍵読出部303、復号文生成部306、復号文検査部307に対して、1つの鍵の読み出し(ステップS1805)と、暗号化スクランブルキーの復号(ステップS1806)と、暗号化スクランブルキーを復号して得られた復号文の検査(ステップS1807～ステップS1809)とを繰り返すように制御する(ステップS1804～ステップS1810)。上記の繰り返しが終了すると、R個の鍵から、暗号化スクランブルキーを正しく復号する1つの鍵が選択され、復号文検査部307は、スクランブルキーをデジタルデータ復号部309へ出力する。次に、デジタルデータ読出部308は、暗号化デジタル著作物を読み出し、デジタルデータ復号部309は、復号文検査部307から受け取ったスクランブルキーを用いて、DES復号アルゴリズムにより、デジタルデータ読出部308により読み出された暗号化デジタル著作物を復号して、デジタル著作物を生成し、生成されたデジタル著作物を表示部310へ出力し(ステップS1811)、表示部310は、デジタルデータ復号部309から出力される64ビットのデジタルデータを繰り返し受け取り、順次表示する(ステップS1812)。

【0078】2. その他の実施の形態

なお、本発明を上記実施の形態に基づいて説明してきたが、本発明は上記実施の形態に限定されないのはもちろんである。すなわち、以下のような場合も本発明に含まれる。

(1) 本実施の形態では、復号鍵候補の決定のために、64ビットのスクランブルキーの先頭に64ビットの連続する0を付加して暗号化し、復号時に先頭64ビットが0であるかどうかを検査するとしているが、これに限定されるものではない。暗号装置において、64ビットのスクランブルキーを暗号化し、引き続き、固定的な情報の暗号化を行ってN個の暗号化固定情報を生成し、復号装置においては、識別番号により識別される暗号化固

定情報を復号して、その復号文が固定的な情報になるかどうかにより判断するとしてもよい。また、鍵管理装置においては、N個の暗号化固定情報を復号して、その復号文が固定的な情報になるかどうかにより判断するとしてもよい。

【0079】(2) 暗号鍵生成部113は、復号鍵セットに含まれるR個の鍵から、1個の鍵をランダムに選択し、選択した1個の鍵を暗号鍵テーブル114の暗号鍵セットに書き込むとしているが、暗号鍵生成部113は、復号鍵セットに含まれるR個の鍵から、一様に1個の鍵をランダムに選択し、選択した1個の鍵を暗号鍵テーブル114の暗号鍵セットに書き込むとしてもよい。ここで、一様に1個の鍵Kをランダムに選択するとは、Kを確率変数とすると、Kのとり得る範囲内で、確率密度関数 $f(K) = \text{一定値を満すように}$ 、Kをランダムに選択することを言う。

【0080】(3) 鍵管理装置100は、暗号鍵セット記録媒体21を各暗号装置に配布し、復号鍵セット記録媒体22を各復号装置に配布するとしているが、前記記録媒体を配布する代わりに、鍵管理装置100と各暗号装置を通信回線で結び、暗号鍵セット記録媒体21に記録されている情報を前記通信回線を経由して、鍵管理装置100から各暗号装置に送信するようにし、また、鍵管理装置100と各復号装置を通信回線で結び、復号鍵セット記録媒体22に記録されている情報を前記通信回線を経由して、鍵管理装置100から各復号装置に送信するようにしてもよい。

【0081】(4) 本実施の形態では、DESを使用しているが、他の暗号アルゴリズムを使用してもよい。

【0082】

【発明の効果】上記に説明するように、本発明は、1台の鍵管理装置と、M(Mは2以上の整数)種類の暗号装置と、N(Nは2以上の整数)種類の復号装置とからなる暗号システムであって、前記鍵管理装置は、復号鍵セットをN個記憶し、暗号鍵セットをM個記憶し、N個の識別番号を記憶し、前記M個の暗号鍵セットをそれぞれ前記M種類の暗号装置に配布し、前記N個の復号鍵セットをそれぞれ前記N種類の復号装置に配布し、前記N個の識別番号をそれぞれ前記N種類の復号装置に配布し、前記暗号鍵セットはN個の暗号鍵からなり、前記復号鍵セットは所定数の復号鍵からなり、前記M種類の暗号装置のそれぞれは、デジタルデータをスクランブルキーを用いて暗号化して暗号化デジタルデータを生成し、前記配布された暗号鍵セットを用いて前記スクランブルキーを暗号化してN個の暗号化スクランブルキーを生成し、前記暗号化デジタルデータと前記N個の暗号化スクランブルキーとを配布媒体に書き込み、前記N種類の復号装置のそれぞれは、前記配布された復号鍵セットに含まれる前記所定数の復号鍵を用いて、前記配布媒体に含まれる前記配布された識別番号により特定される1つの暗号化

スクランブルキーを順次復号し、第1の所定の基準により正しく復号されたスクランブルキーを用いて前記配布媒体に含まれる暗号化デジタルデータを復号してデジタルデータを生成し、識別番号は、配布媒体に書き込まれているN個の暗号化スクランブルキーから当該復号装置に対応する1つの暗号化スクランブルキーを識別し、前記鍵管理装置は、さらに、前記配布媒体から1つの暗号化スクランブルキーを読み出す第1暗号文読出手段と、1つの復号鍵セットを読み出す復号鍵セット読出手段と、前記読み出した復号鍵セットに含まれる前記所定数の復号鍵を用いて、前記読み出した暗号化スクランブルキーを順次復号し、前記第1の所定の基準により正しく暗号化スクランブルキーを復号する復号鍵を、前記所定数の復号鍵の中から1つ選択する復号鍵選択手段と、前記配布媒体からN個の暗号化スクランブルキーの読み出しが終了するまで、前記第1暗号文読出手段、前記復号鍵セット読出手段、前記復号鍵選択手段に対して、暗号化スクランブルキーの読み出しと、復号鍵セットの読み出しと、読み出した暗号化スクランブルキーの復号とを繰り返し行うように制御し、その結果N個の復号鍵のセットが選択される第1繰返制御手段と、前記M個の暗号鍵セットから、前記選択されたN個の復号鍵のセットと一致する1つの暗号鍵セットを検出し、検出された暗号鍵セットにより特定される暗号装置を識別する鍵パターン検出手段とを備える。この構成によれば、鍵管理装置は、配布媒体がどの種類の暗号装置により生産されたものであるかを識別することができるという効果がある。

【0083】ここで、前記鍵管理装置は、所定数の復号鍵からなる復号鍵セットをN個記憶している第1復号鍵記憶手段と、前記第1復号鍵記憶手段に記憶されているN個の復号鍵セットのそれぞれから、第1の所定の方法により1つの復号鍵を選択して1つの暗号鍵とし、N個の暗号鍵からなる暗号鍵セットを生成する暗号鍵生成手段と、前記生成された1つの暗号鍵セットを記憶する第1暗号鍵記憶手段と、M個の暗号鍵セットが生成されるまで、前記暗号鍵生成手段に対して、暗号鍵セットの生成を繰り返すように制御し、その結果、前記第1暗号鍵記憶手段はM個の暗号鍵セットを記憶する第2繰返制御手段と、前記第1暗号鍵記憶手段に記憶されているM個の暗号鍵セットをそれぞれ前記M種類の暗号装置に配布する暗号鍵セット配布手段と、前記第1復号鍵記憶手段に記憶されているN個の復号鍵セットをそれぞれ前記N種類の復号装置に配布する復号鍵セット配布手段と、N個の識別番号をそれぞれ前記N種類の復号装置に配布する識別番号配布手段とを備えるように構成してもよい。この構成によれば、各復号装置には、異なる復号鍵が割り当てられるので、暗号が解読されにくいという効果がある。また、万一ある復号装置が解析され、内部に格納されている復号鍵が見破られたとしても、その復号鍵を他の復号装置に用いることができず、他の復号装置に影響

を与えないという効果がある。

【0084】ここで、前記第1の所定の方法とは、前記第1復号鍵記憶手段に記憶されているN個の復号鍵セットのそれぞれから、ランダムに1個の復号鍵を選択することであるように構成してもよい。この構成によれば、暗号装置に割り当てられるN個の暗号鍵は、各復号装置に割り当てられる所定数の復号鍵のうちの1つをランダムに選択するので、異なる暗号鍵の組合せが多くなり、異なる暗号鍵を割り当てることのできる暗号装置の数を多くすることができるという効果がある。

【0085】ここで、前記第1の所定の方法とは、前記第1復号鍵記憶手段に記憶されているN個の復号鍵セットのそれぞれから、一様にランダムに1個の復号鍵を選択することであるように構成してもよい。この構成によれば、暗号装置に割り当てられるN個の暗号鍵は、各復号装置に割り当てられる所定数の復号鍵から一様にランダムに選択するので、どれか1つの種類の暗号装置が記憶する暗号鍵が暴露されたとしても、全体の暗号鍵が暴露されることがないという効果がある。

【0086】ここで、前記M種類の暗号装置のそれぞれは、前記鍵管理装置から配布された1つの暗号鍵セットを受信し、受信した前記暗号鍵セットを記憶する第2暗号鍵記憶手段と、スクランブルキーを生成するスクランブルキー生成手段と、外部からデジタルデータを受信し、受信したデジタルデータを前記生成されたスクランブルキーを用いて暗号化し、暗号化デジタルデータを生成するデジタルデータ暗号化手段と、前記第2暗号鍵記憶手段に記憶されている暗号鍵セットに含まれるN個の暗号鍵を用いて、第2の所定の方法により、前記スクランブルキーを順次暗号化し、N個の暗号化スクランブルキーを生成する鍵暗号化手段と、前記生成された暗号化デジタルデータと前記生成されたN個の暗号化スクランブルキーとを配布媒体に書き込む媒体書込手段とを備えるように構成してもよい。この構成によれば、暗号装置は、各復号装置毎に、スクランブルキーを暗号化し、各復号装置は、割り当てられた復号鍵でスクランブルキーを復号するので、暗号が解読されにくいという効果がある。

【0087】ここで、前記第2の所定の方法とは、前記スクランブルキーと固定値からなる固定情報とを結合し、結合されたスクランブルキーと固定情報とを暗号化することであるように構成してもよい。この構成によれば、暗号装置において暗号文を生成する際に、平文と固定値からなる固定情報とを結合し、結合された平文と固定情報とを暗号化し、復号装置において、暗号文を復号する際に、前記固定情報が生成されることにより、暗号文が正しく復号されたと判定する。このように、簡単な方法により鍵の決定ができるという効果がある。

【0088】ここで、前記第2の所定の方法とは、前記スクランブルキーを暗号化してN個の暗号化スクランブ

ルキーを生成し、さらに、固定値からなる固定情報を暗号化してN個の暗号化固定情報を生成することであり、前記媒体書込手段は、暗号化デジタルデータとN個の暗号化スクランブルキーとN個の暗号化固定情報とを配布媒体に書き込むように構成してもよい。この構成によれば、暗号装置において暗号文を生成する際に、さらに固定値からなる固定情報を暗号化して暗号化固定情報を生成し、復号装置において、暗号文を復号する際に、前記暗号化固定情報が復号されて、固定情報が生成されることにより、暗号文が正しく復号されたと判定する。このように、簡単な方法により鍵の決定ができるという効果がある。

【0089】ここで、前記復号選択手段は、前記復号鍵セットから復号鍵を順次読み出す第1復号鍵読出手段と、前記読み出した復号鍵を用いて、前記読み出した暗号化スクランブルキーを復号し、復号文を生成する第1復号文生成手段と、前記第1の所定の基準により、復号文が正しく復号されているかどうかを検査する第1復号文検査手段と、前記復号鍵セットから所定数の復号鍵の読出しが終了するまで、前記第1復号鍵読出手段、前記第1復号文生成手段、前記第1復号文検査手段に対して、復号鍵の読出しと、暗号化スクランブルキーの復号と、復号文の検査とを繰り返し行うように制御する第3繰返制御手段と、前記復号文検査手段により正しく復号されたと検査された際に用いられた復号鍵を出力する鍵出力手段とを備えるように構成してもよい。この構成によれば、鍵管理装置は、配布媒体がどの種類の暗号装置により生産されたものであるかを識別することができるという効果がある。

【0090】ここで、前記第1の所定の基準とは、前記復号文に固定値からなる固定情報が含まれることであるように構成してもよい。この構成によれば、暗号装置において暗号文を生成する際に、平文と固定値からなる固定情報とを結合し、結合された平文と固定情報とを暗号化し、復号装置において、暗号文を復号する際に、前記固定情報が生成されることにより、暗号文が正しく復号されたと判定する。このように、簡単な方法により鍵の決定ができるという効果がある。

【0091】ここで、前記配布媒体は、さらに、前記暗号鍵セットに含まれるN個の暗号鍵を用いて固定値からなる固定情報が暗号化されたN個の暗号化固定情報を含み、前記鍵管理装置は、さらに、N個の暗号化固定情報を読み出す暗号化固定情報読出手段と、前記N個の復号鍵セットを用いて、前記読み出したN個の暗号化固定情報をそれぞれ復号する暗号化固定情報復号手段とを含み、前記第1の所定の基準とは、暗号化固定情報を復号して復号文を生成し、生成された復号文に固定値からなる固定情報が含まれることであるように構成してもよい。この構成によれば、暗号装置において暗号文を生成する際に、さらに固定値からなる固定情報を暗号化して

暗号化固定情報を生成し、復号装置において、暗号文を復号する際に、前記暗号化固定情報が復号されて、固定情報が生成されることにより、暗号文が正しく復号されたと判定する。このように、簡単な方法により鍵の決定ができるという効果がある。

【0092】ここで、前記N種類の復号装置のそれぞれは、前記鍵管理装置から識別番号を受信し、受信した識別番号を記憶する識別番号記憶手段と、前記鍵管理装置から配布された1つの復号鍵セットを受信し、受信した前記復号鍵セットを記憶する第2復号鍵記憶手段と、前記配布媒体から前記受信した識別番号により識別される1つの暗号化スクランブルキーを読み出す第2暗号文読出手段と、前記配布媒体から暗号化デジタルデータを読み出すデジタルデータ読出手段と、前記第2復号鍵記憶手段から前記復号鍵セットに含まれる復号鍵を順次読み出す第2復号鍵読出手段と、前記読み出した復号鍵を用いて、前記読み出した暗号化スクランブルキーを復号し、復号文を生成する第2復号文生成手段と、前記第1の所定の基準により、復号文が正しく復号されているかどうかを検査し、正しく復号された場合に前記復号文をスクランブルキーとする第2復号文検査手段と、復号鍵セットから所定数の復号鍵の読出しが終了するまで、前記第2復号鍵読出手段、前記第2復号文生成手段、前記第2復号文検査手段に対して、復号鍵の読出しと、暗号化スクランブルキーの復号と、復号文の検査とを繰り返し行うように制御する第4繰返制御手段と、前記復号文検査手段により正しく復号されたと検査されたスクランブルキーを用いて、前記読み出した暗号化デジタルデータを復号し、デジタルデータを生成するデジタルデータ復号手段とを備えるように構成してもよい。この構成によれば、鍵管理装置は、復号装置に対して、暗号装置が作成したN個の暗号文のうち、その復号装置に対応する暗号文を識別する情報を予め通知し、復号装置はこの情報を用いて暗号文を識別することができるという効果がある。

【0093】ここで、前記第1の所定の基準とは、前記復号文に固定値からなる固定情報が含まれることであるように構成してもよい。この構成によれば、暗号装置において暗号文を生成する際に、平文と固定値からなる固定情報とを結合し、結合された平文と固定情報とを暗号化し、復号装置において、暗号文を復号する際に、前記固定情報が生成されることにより、暗号文が正しく復号されたと判定する。このように、簡単な方法により鍵の決定ができるという効果がある。

【0094】ここで、前記配布媒体は、さらに、前記暗号鍵セットに含まれるN個の暗号鍵を用いて固定値からなる固定情報が暗号化されたN個の暗号化固定情報を含み、前記復号装置は、さらに、前記識別番号により識別される1つの暗号化固定情報を読み出す暗号化固定情報読出手段と、前記復号鍵セットに含まれる所定数の復号

鍵を用いて、前記読み出した暗号化固定情報を復号する暗号化固定情報復号手段とを備え、前記第 1 の所定の基準とは、暗号化固定情報を復号して復号文を生成し、生成された復号文に固定値からなる固定情報が含まれることであるように構成してもよい。この構成によれば、暗号装置において暗号文を生成する際に、さらに固定値からなる固定情報を暗号化して暗号化固定情報を生成し、復号装置において、暗号文を復号する際に、前記暗号化固定情報が復号されて、固定情報が生成されることにより、暗号文が正しく復号されたと判定する。このように、簡単な方法により鍵の決定ができるという効果がある。

【0095】ここで、前記M種類の暗号装置のそれぞれは、前記鍵管理装置から配布された 1 つの暗号鍵セットを受信し、受信した前記暗号鍵セットを記憶する第 2 暗号鍵記憶手段と、スクランブルキーを生成するスクランブルキー生成手段と、外部からデジタルデータを受信し、受信したデジタルデータを前記生成されたスクランブルキーを用いて暗号化し、暗号化デジタルデータを生成するデジタルデータ暗号化手段と、前記第 2 暗号鍵記憶手段に記憶されている暗号鍵セットに含まれるN個の暗号鍵を用いて、第 2 の所定の方法により、前記スクランブルキーを順次暗号化し、N個の暗号化スクランブルキーを生成する鍵暗号化手段と、前記生成された暗号化デジタルデータと前記生成されたN個の暗号化スクランブルキーとを配布媒体に書き込む媒体書込手段とを備え、前記鍵管理装置において、前記復号選択手段は、前記復号鍵セットから復号鍵を順次読み出す第 1 復号鍵読出手段と、前記読み出した復号鍵を用いて、前記読み出した暗号化スクランブルキーを復号し、復号文を生成する第 1 復号文生成手段と、前記第 1 の所定の基準により、復号文が正しく復号されているかどうかを検査する第 1 復号文検査手段と、前記復号鍵セットから所定数の復号鍵の読出しが終了するまで、前記第 1 復号鍵読出手段、前記第 1 復号文生成手段、前記第 1 復号文検査手段に対して、復号鍵の読出しと、暗号化スクランブルキーの復号と、復号文の検査とを繰り返すように制御する第 3 繰返制御手段と、前記復号文検査手段により正しく復号されたと検査された際に用いられた復号鍵を出力する鍵出力手段とを備えるように構成してもよい。この構成によれば、暗号装置は、各復号装置毎にスクランブルキーを暗号化し、鍵管理装置は、配布媒体がどの種類の暗号装置により生産されたものであるかを識別することができるという効果がある。

【0096】ここで、前記第 1 の所定の基準とは、前記復号文に固定情報が含まれることであり、前記第 2 の所定の方法とは、前記スクランブルキーと固定値からなる固定情報とを結合し、結合されたスクランブルキーと固定情報とを暗号化することであるように構成してもよい。この構成によれば、暗号装置において暗号文を生成

する際に、平文と固定値からなる固定情報とを結合し、結合された平文と固定情報とを暗号化し、復号装置において、暗号文を復号する際に、前記固定情報が生成されることにより、暗号文が正しく復号されたと判定する。このように、簡単な方法により鍵の決定ができるという効果がある。

【0097】ここで、前記第 2 の所定の方法とは、前記スクランブルキーを暗号化してN個の暗号化スクランブルキーを生成し、さらに、固定値からなる固定情報を暗号化してN個の暗号化固定情報を生成することであり、前記媒体書込手段は、暗号化デジタルデータとN個の暗号化スクランブルキーとN個の暗号化固定情報とを配布媒体に書き込み、前記鍵管理装置は、N個の暗号化固定情報を読み出す暗号化固定情報読出手段と、N個の復号鍵セットを用いて、前記読み出したN個の暗号化固定情報をそれぞれ復号する暗号化固定情報復号手段とを備え、前記第 1 の所定の基準とは、N個の暗号化固定情報を復号し、さらに、固定情報を生成することであるように構成してもよい。この構成によれば、暗号装置において暗号文を生成する際に、さらに固定値からなる固定情報を暗号化して暗号化固定情報を生成し、復号装置において、暗号文を復号する際に、前記暗号化固定情報が復号されて、固定情報が生成されることにより、暗号文が正しく復号されたと判定する。このように、簡単な方法により鍵の決定ができるという効果がある。

【0098】ここで、前記M種類の暗号装置のそれぞれは、前記鍵管理装置から配布された 1 つの暗号鍵セットを受信し、受信した前記暗号鍵セットを記憶する第 2 暗号鍵記憶手段と、スクランブルキーを生成するスクランブルキー生成手段と、外部からデジタルデータを受信し、受信したデジタルデータを前記生成されたスクランブルキーを用いて暗号化し、暗号化デジタルデータを生成するデジタルデータ暗号化手段と、前記第 2 暗号鍵記憶手段に記憶されている暗号鍵セットに含まれるN個の暗号鍵を用いて、第 2 の所定の方法により、前記スクランブルキーを順次暗号化し、N個の暗号化スクランブルキーを生成する鍵暗号化手段と、前記生成された暗号化デジタルデータと前記生成されたN個の暗号化スクランブルキーとを配布媒体に書き込む媒体書込手段とを備え、前記N種類の復号装置のそれぞれは、前記鍵管理装置から識別番号を受信し、受信した識別番号を記憶する識別番号記憶手段と、前記鍵管理装置から配布された 1 つの復号鍵セットを受信し、受信した前記復号鍵セットを記憶する第 2 復号鍵記憶手段と、前記配布媒体から前記受信した識別番号により識別される 1 つの暗号化スクランブルキーを読み出す第 2 暗号文読出手段と、前記配布媒体から暗号化デジタルデータを読み出すデジタルデータ読出手段と、前記第 2 復号鍵記憶手段から前記復号鍵セットに含まれる復号鍵を順次読み出す第 2 復号鍵読出手段と、前記読み出した復号鍵を用いて、前記読み出

した暗号化スクランブルキーを復号し、復号文を生成する第2復号文生成手段と、前記第1の所定の基準により、復号文が正しく復号されているかどうかを検査し、正しく復号された場合に前記復号文はスクランブルキーを含む第2復号文検査手段と、復号鍵セットから所定数の復号鍵の読出しが終了するまで、前記第2復号鍵読出手段、前記第2復号文生成手段、前記第2復号文検査手段に対して、復号鍵の読出しと、暗号化スクランブルキーの復号と、復号文の検査とを繰り返し行うように制御する第4繰返制御手段と、前記復号文検査手段により正しく復号されたと検査されたスクランブルキーを用いて、前記読み出した暗号化デジタルデータを復号し、デジタルデータを生成するデジタルデータ復号手段とを備えるように構成してもよい。この構成によれば、各復号装置には、異なる復号鍵が割り当てられるので、暗号が解読されにくいという効果がある。また、万一ある復号装置が解析され、内部に格納されている復号鍵が見破られたとしても、その復号鍵を他の復号装置に用いることができず、他の復号装置に影響を与えないという効果がある。

【0099】ここで、前記第1の所定の基準とは、前記復号文に固定情報が含まれることであり、前記第2の所定の方法とは、前記スクランブルキーと固定値からなる固定情報とを結合し、結合されたスクランブルキーと固定情報とを暗号化することであるように構成してもよい。この構成によれば、暗号装置において暗号文を生成する際に、平文と固定値からなる固定情報とを結合し、結合された平文と固定情報とを暗号化し、復号装置において、暗号文を復号する際に、前記固定情報が生成されることにより、暗号文が正しく復号されたと判定する。このように、簡単な方法により鍵の決定ができるという効果がある。

【0100】ここで、前記第2の所定の方法とは、前記スクランブルキーを暗号化してN個の暗号化スクランブルキーを生成し、さらに、固定値からなる固定情報を暗号化してN個の暗号化固定情報を生成することであり、前記媒体書込手段は、暗号化デジタルデータとN個の暗号化スクランブルキーとN個の暗号化固定情報とを配布媒体に書き込み、前記復号装置は、さらに、前記識別番号により識別される暗号化固定情報を読み出す暗号化固定情報読出手段と、復号鍵セットに含まれる所定数の復号鍵を用いて、前記読み出した暗号化固定情報を読み出す暗号化固定情報復号手段とを備え、前記第1の所定の基準とは、暗号化固定情報を復号し、さらに、固定情報を生成することであるように構成してもよい。この構成によれば、暗号装置において暗号文を生成する際に、さらに固定値からなる固定情報を暗号化して暗号化固定情報を生成し、復号装置において、暗号文を復号する際に、前記暗号化固定情報が復号されて、固定情報が生成されることにより、暗号文が正しく復号されたと判定す

る。このように、簡単な方法により鍵の決定ができるという効果がある。

【0101】ここで、前記鍵管理装置は、所定数の復号鍵からなる復号鍵セットをN個記憶している第1復号鍵記憶手段と、前記第1復号鍵記憶手段に記憶されているN個の復号鍵セットのそれぞれから、第1の所定の方法により1つの復号鍵を選択して1つの暗号鍵とし、N個の暗号鍵からなる暗号鍵セットを生成する暗号鍵生成手段と、前記生成された1つの暗号鍵セットを記憶する第1暗号鍵記憶手段と、M個の暗号鍵セットが生成されるまで、前記暗号鍵生成手段に対して、暗号鍵セットの生成を繰り返すように制御し、この結果、前記第1暗号鍵記憶手段はM個の暗号鍵セットを記憶する第2繰返制御手段と、前記第1暗号鍵記憶手段に記憶されているM個の暗号鍵セットをそれぞれ前記M種類の暗号装置に配布する暗号鍵セット配布手段と、前記第1復号鍵記憶手段に記憶されているN個の復号鍵セットをそれぞれ前記N種類の復号装置に配布する復号鍵セット配布手段と、識別番号を前記N種類の復号装置に配布する識別番号配布手段とを備え、前記N種類の復号装置のそれぞれは、前記鍵管理装置から識別番号を受信し、受信した識別番号を記憶する識別番号記憶手段と、前記鍵管理装置から配布された1つの復号鍵セットを受信し、受信した前記復号鍵セットを記憶する第2復号鍵記憶手段と、前記配布媒体から前記受信した識別番号により識別される1つの暗号化スクランブルキーを読み出す第2暗号文読出手段と、前記配布媒体から暗号化デジタルデータを読み出すデジタルデータ読出手段と、前記第2復号鍵記憶手段から前記復号鍵セットに含まれる復号鍵を順次読み出す第2復号鍵読出手段と、前記読み出した復号鍵を用いて、前記読み出した暗号化スクランブルキーを復号し、復号文を生成する第2復号文生成手段と、前記第1の所定の基準により、復号文が正しく復号されているかどうかを検査し、正しく復号された場合に前記復号文をスクランブルキーとする第2復号文検査手段と、復号鍵セットから所定数の復号鍵の読出しが終了するまで、前記第2復号鍵読出手段、前記第2復号文生成手段、前記第2復号文検査手段に対して、復号鍵の読出しと、暗号化スクランブルキーの復号と、復号文の検査とを繰り返し行うように制御する第4繰返制御手段と、前記復号文検査手段により正しく復号されたと検査されたスクランブルキーを用いて、前記読み出した暗号化デジタルデータを復号し、デジタルデータを生成するデジタルデータ復号手段とを備えるように構成してもよい。この構成によれば、各復号装置には、異なる復号鍵が割り当てられるので、暗号が解読されにくいという効果がある。また、万一ある復号装置が解析され、内部に格納されている復号鍵が見破られたとしても、その復号鍵を他の復号装置に用いることができず、他の復号装置に影響を与えないという効果がある。また、鍵管理装置は、復号装置に対して、

暗号装置が作成したN個の暗号文のうち、その復号装置に対応する暗号文を識別する情報を予め通知し、復号装置はこの情報を用いて暗号文を識別することができるという効果がある。

【0102】ここで、前記第1の所定の方法とは、前記第1復号鍵記憶手段に記憶されているN個の復号鍵セットのそれぞれから、ランダムに1個の復号鍵を選択することであるように構成してもよい。この構成によれば、暗号装置に割り当てられるN個の暗号鍵は、各復号装置に割り当てられる所定数の復号鍵のうちの1つをランダムに選択するので、異なる暗号鍵の組合せが多くなり、異なる暗号鍵を割り当てることができる暗号装置の数を多くすることができるという効果がある。

【0103】ここで、前記第1の所定の方法とは、前記第1復号鍵記憶手段に記憶されているN個の復号鍵セットのそれぞれから、一様にランダムに1個の復号鍵を選択することであるように構成してもよい。この構成によれば、暗号装置に割り当てられるN個の暗号鍵は、各復号装置に割り当てられる所定数の復号鍵から一様にランダムに選択するので、どれか1つの種類の暗号装置が記憶する暗号鍵が暴露されたとしても、全体の暗号鍵が暴露されることがないという効果がある。

【0104】ここで、前記第1の所定の基準とは、前記復号文に固定値からなる固定情報が含まれることであるように構成してもよい。この構成によれば、暗号装置において暗号文を生成する際に、平文と固定値からなる固定情報とを結合し、結合された平文と固定情報とを暗号化し、復号装置において、暗号文を復号する際に、前記固定情報が生成されることにより、暗号文が正しく復号されたと判定する。このように、簡単な方法により鍵の決定ができるという効果がある。

【0105】ここで、前記配布媒体は、さらに、前記暗号鍵セットに含まれるN個の暗号鍵を用いて固定値からなる固定情報が暗号化されたN個の暗号化固定情報を含み、前記復号装置は、さらに、前記識別番号により識別される1つの暗号化固定情報を読み出す暗号化固定情報読出手段と、前記復号鍵セットに含まれる所定数の復号鍵を用いて、前記読み出した暗号化固定情報を復号する暗号化固定情報復号手段とを備え、前記第1の所定の基準とは、暗号化固定情報を復号して復号文を生成し、生成された復号文に固定値からなる固定情報が含まれることであるように構成してもよい。この構成によれば、暗号装置において暗号文を生成する際に、さらに固定値からなる固定情報を暗号化して暗号化固定情報を生成し、復号装置において、暗号文を復号する際に、前記暗号化固定情報が復号されて、固定情報が生成されることにより、暗号文が正しく復号されたと判定する。このように、簡単な方法により鍵の決定ができるという効果がある。

【0106】また、本発明は、M (Mは2以上の整数)

種類の暗号装置とN (Nは2以上の整数) 種類の復号装置に鍵情報を配布する鍵管理装置であって、所定数の復号鍵からなる復号鍵セットをN個記憶している復号鍵記憶手段と、前記復号鍵記憶手段に記憶されているN個の復号鍵セットのそれぞれから、第1の所定の方法により1つの復号鍵を選択して1つの暗号鍵とし、N個の暗号鍵からなる暗号鍵セットを生成する暗号鍵生成手段と、前記生成された1つの暗号鍵セットを記憶する暗号鍵記憶手段と、M個の暗号鍵セットが生成されるまで、前記暗号鍵生成手段に対して、暗号鍵セットの生成を繰り返すように制御し、その結果、前記暗号鍵記憶手段はM個の暗号鍵セットを記憶する繰返制御手段と、前記第1暗号鍵記憶手段に記憶されているM個の暗号鍵セットをそれぞれM種類の暗号装置に配布する暗号鍵セット配布手段と、前記第1復号鍵記憶手段に記憶されているN個の復号鍵セットをそれぞれN種類の復号装置に配布する復号鍵セット配布手段と、N個の識別番号をそれぞれN種類の復号装置に配布する識別番号配布手段とを備える。この構成によれば、各復号装置には、異なる復号鍵が割り当てられるので、暗号が解読されにくいという効果がある。また、万一ある復号装置が解析され、内部に格納されている復号鍵が見破られたとしても、その復号鍵を他の復号装置に用いることができず、他の復号装置に影響を与えないという効果がある。

【0107】また、本発明は、鍵管理装置から配布される鍵情報を用いて、デジタルデータを暗号化して配布媒体に書き込む暗号装置であって、鍵管理装置から配布された1つの暗号鍵セットを受信し、受信した前記暗号鍵セットを記憶する暗号鍵記憶手段と、スクランブルキーを生成するスクランブルキー生成手段と、外部からデジタルデータを受信し、受信したデジタルデータを前記生成されたスクランブルキーを用いて暗号化し、暗号化デジタルデータを生成するデジタルデータ暗号化手段と、前記暗号鍵記憶手段に記憶されている暗号鍵セットに含まれるN (Nは2以上の整数) 個の暗号鍵を用いて、所定の方法により、前記スクランブルキーを順次暗号化し、N個の暗号化スクランブルキーを生成する鍵暗号化手段と、前記生成された暗号化デジタルデータと前記生成されたN個の暗号化スクランブルキーとを配布媒体に書き込む媒体書込手段とを備える。この構成によれば、暗号装置は、各復号装置毎に、スクランブルキーを暗号化し、各復号装置は、異なる復号鍵が割り当てられるので、暗号が解読されにくいという効果がある。また、万一ある復号装置が解析され、内部に格納されている復号鍵が見破られたとしても、その復号鍵を他の復号装置に用いることができず、他の復号装置に影響を与えないという効果がある。

【0108】また、本発明は、鍵管理装置から配布された鍵情報を用いて、配布媒体に書かれた暗号化デジタルデータを復号する復号装置であって、配布媒体に書き込

まれているN個の暗号化スクランブルキーから当該復号装置に対応する1つの暗号化スクランブルキーを識別する識別番号を鍵管理装置から受信し、受信した識別番号を記憶する識別番号記憶手段と、鍵管理装置から配布された1つの復号鍵セットを受信し、受信した前記復号鍵セットを記憶する復号鍵記憶手段と、前記配布媒体から前記受信した識別番号により識別される1つの暗号化スクランブルキーを読み出す暗号文読出手段と、前記配布媒体から暗号化デジタルデータを読み出すデジタルデータ読出手段と、前記復号鍵記憶手段から前記復号鍵セットに含まれる復号鍵を順次読み出す復号鍵読出手段と、前記読み出した復号鍵を用いて、前記読み出した暗号化スクランブルキーを復号し、復号文を生成する復号文生成手段と、所定の基準により、復号文が正しく復号されているかどうかを検査し、正しく復号された場合に前記復号文はスクランブルキーを含む復号文検査手段と、復号鍵セットから所定数の復号鍵の読出しが終了するまで、前記復号鍵読出手段、前記復号文生成手段、前記復号文検査手段に対して、復号鍵の読出しと、暗号化スクランブルキーの復号と、復号文の検査とを繰り返し行うように制御する繰返制御手段と、前記復号文検査手段により正しく復号されたと検査されたスクランブルキーを用いて、前記読み出した暗号化デジタルデータを復号し、デジタルデータを生成するデジタルデータ復号手段とを備える。この構成によれば、各復号装置には、異なる復号鍵が割り当てられるので、暗号が解読されにくいという効果がある。また、万一ある復号装置が解析され、内部に格納されている復号鍵が見破られたとしても、その復号鍵を他の復号装置に用いることができず、他の復号装置に影響を与えないという効果がある。

【0109】また、本発明は、配布媒体にデジタルデータを暗号化して書き込んだ暗号装置の種類を識別する鍵管理装置であって、前記配布媒体から1つの暗号化スクランブルキーを読み出す暗号文読出手段と、1つの復号鍵セットを読み出す復号鍵セット読出手段と、前記読み出した復号鍵セットに含まれる所定数の復号鍵を用いて、前記読み出した暗号化スクランブルキーを順次復号し、所定の基準により正しく暗号化スクランブルキーを復号する復号鍵を、前記所定数の復号鍵の中から1つ選択する復号選択手段と、前記配布媒体からN個の暗号化スクランブルキーの読み出しが終了するまで、前記暗号文読出手段、前記復号鍵セット読出手段、前記復号選択手段に対して、暗号化スクランブルキーの読み出しと、復号鍵セットの読み出しと、読み出した暗号化スクランブルキーの復号とを繰り返し行うように制御し、この結果、N個の復号鍵のセットが選択される繰返制御手段と、前記M個の暗号鍵セットから、前記選択されたN個の復号鍵のセットと一致する1つの暗号鍵セットを検出し、検出された暗号鍵セットにより特定される暗号装置を識別する鍵パターン検出手段とを備える。この構成に

よれば、鍵管理装置は、配布媒体がどの種類の暗号装置により生産されたものであるかを識別することができるという効果がある。

【0110】また、本発明は、M (Mは2以上の整数) 種類の暗号装置とN (Nは2以上の整数) 種類の復号装置に鍵情報を配布し、所定数の復号鍵からなる復号鍵セットをN個記憶している復号鍵記憶手段を備える鍵管理装置において用いられる鍵管理方法であって、前記復号鍵記憶手段に記憶されているN個の復号鍵セットのそれぞれから、所定の方法により1つの復号鍵を選択して1つの暗号鍵とし、N個の暗号鍵からなる暗号鍵セットを生成する暗号鍵生成ステップと、M個の暗号鍵セットが生成されるまで、前記暗号鍵生成ステップに対して、暗号鍵セットの生成を繰り返すように制御し、この結果、M個の暗号鍵セットが生成される繰返制御ステップと、暗号鍵生成ステップにより生成されたM個の暗号鍵セットをそれぞれM種類の暗号装置に配布する暗号鍵セット配布ステップと、前記復号鍵記憶手段に記憶されているN個の復号鍵セットをそれぞれN種類の復号装置に配布する復号鍵セット配布ステップと、N個の識別番号をそれぞれN種類の復号装置に配布する識別番号配布ステップとを含む。この方法を用いると、各復号装置には、異なる復号鍵が割り当てられるので、暗号が解読されにくいという効果がある。また、万一ある復号装置が解析され、内部に格納されている復号鍵が見破られたとしても、その復号鍵を他の復号装置に用いることができず、他の復号装置に影響を与えないという効果がある。

【0111】ここで、前記所定の方法とは、前記復号鍵記憶手段に記憶されているN個の復号鍵セットのそれぞれから、ランダムに1個の復号鍵を選択することであるように構成してもよい。この方法を用いると、暗号装置に割り当てられるN個の暗号鍵は、各復号装置に割り当てられる所定数の復号鍵のうちの1つをランダムに選択するので、異なる暗号鍵の組合せが多くなり、異なる暗号鍵を割り当てることのできる暗号装置の数を多くすることができるという効果がある。

【0112】ここで、前記所定の方法とは、前記復号鍵記憶手段に記憶されているN個の復号鍵セットのそれぞれから、一様にランダムに1個の復号鍵を選択することであるように構成してもよい。この方法を用いると、暗号装置に割り当てられるN個の暗号鍵は、各復号装置に割り当てられる所定数の復号鍵から一様にランダムに選択するので、どれか1つの種類の暗号装置が記憶する暗号鍵が暴露されたとしても、全体の暗号鍵が暴露されることがないという効果がある。

【0113】また、本発明は、鍵管理装置から配布される鍵情報を用いて、デジタルデータを暗号化して配布媒体に書き込み、鍵管理装置から配布された1つの暗号鍵セットを受信し受信した前記暗号鍵セットを記憶する暗号鍵記憶手段を備える暗号装置において用いられる暗号

方法であって、スクランブルキーを生成するスクランブルキー生成ステップと、外部からデジタルデータを受信し、受信したデジタルデータを前記生成されたスクランブルキーを用いて暗号化し、暗号化デジタルデータを生成するデジタルデータ暗号化ステップと、前記暗号鍵記憶手段に記憶されている暗号鍵セットに含まれるN（Nは2以上の整数）個の暗号鍵を用いて、所定の方法により、前記スクランブルキーを順次暗号化し、N個の暗号化スクランブルキーを生成する鍵暗号化ステップと、前記生成された暗号化デジタルデータと前記生成されたN個の暗号化スクランブルキーとを配布媒体に書き込む媒体書込ステップとを含む。この方法を用いると、暗号装置は、各復号装置毎にスクランブルキーを暗号化し、各復号装置は、異なる復号鍵が割り当てられるので、暗号が解読されにくいという効果がある。また、万一ある復号装置が解析され、内部に格納されている復号鍵が見破られたとしても、その復号鍵を他の復号装置に用いることができず、他の復号装置に影響を与えないという効果がある。

【0114】ここで、前記所定の方法とは、前記スクランブルキーと固定値からなる固定情報とを結合し、結合されたスクランブルキーと固定情報とを暗号化することであるように構成してもよい。この方法を用いると、暗号装置において暗号文を生成する際に、平文と固定値からなる固定情報とを結合し、結合された平文と固定情報とを暗号化し、復号装置において、暗号文を復号する際に、前記固定情報が生成されることにより、暗号文が正しく復号されたと判定する。このように、簡単な方法により鍵の決定ができるという効果がある。

【0115】ここで、前記所定の方法とは、前記スクランブルキーを暗号化してN個の暗号化スクランブルキーを生成し、さらに、固定値からなる固定情報を暗号化してN個の暗号化固定情報を生成することであり、前記媒体書込ステップは、暗号化デジタルデータとN個の暗号化スクランブルキーとN個の暗号化固定情報とを配布媒体に書き込むように構成してもよい。この方法を用いると、暗号装置において暗号文を生成する際に、さらに固定値からなる固定情報を暗号化して暗号化固定情報を生成し、復号装置において、暗号文を復号する際に、前記暗号化固定情報が復号されて、固定情報が生成されることにより、暗号文が正しく復号されたと判定する。このように、簡単な方法により鍵の決定ができるという効果がある。

【0116】また、本発明は、鍵管理装置から配布された鍵情報を用いて、配布媒体に書かれた暗号化デジタルデータを復号し、鍵管理装置から識別番号を受信し受信した識別番号を記憶する識別番号記憶手段と、鍵管理装置から配布された1つの復号鍵セットを受信し受信した前記復号鍵セットを記憶する復号鍵記憶手段とを備える復号装置において用いられる復号方法であって、前記識

別番号は配布媒体に書き込まれているN個の暗号化スクランブルキーから当該復号装置に対応する1つの暗号化スクランブルキーを識別し、前記配布媒体から前記受信した識別番号により識別される1つの暗号化スクランブルキーを読み出す暗号文読出ステップと、前記配布媒体から暗号化デジタルデータを読み出すデジタルデータ読出ステップと、前記復号鍵記憶手段から前記復号鍵セットに含まれる復号鍵を順次読み出す復号鍵読出ステップと、前記読み出した復号鍵を用いて、前記読み出した暗号化スクランブルキーを復号し、復号文を生成する復号文生成ステップと、所定の基準により、復号文が正しく復号されているかどうかを検査し、正しく復号された場合に前記復号文はスクランブルキーを含む復号文検査ステップと、復号鍵セットから所定数の復号鍵の読出しが終了するまで、前記復号鍵読出ステップ、前記復号文生成ステップ、前記復号文検査ステップに対して、復号鍵の読出しと、暗号化スクランブルキーの復号と、復号文の検査とを繰り返し行うように制御する繰返制御ステップと、前記復号文検査ステップにより正しく復号されたと検査されたスクランブルキーを用いて、前記読み出した暗号化デジタルデータを復号し、デジタルデータを生成するデジタルデータ復号ステップとを含む。この方法を用いると、各復号装置には、異なる復号鍵が割り当てられるので、暗号が解読されにくいという効果がある。また、万一ある復号装置が解析され、内部に格納されている復号鍵が見破られたとしても、その復号鍵を他の復号装置に用いることができず、他の復号装置に影響を与えないという効果がある。

【0117】ここで、前記所定の基準とは、前記復号文に固定値からなる固定情報が含まれることであるように構成してもよい。この方法を用いると、暗号装置において暗号文を生成する際に、平文と固定値からなる固定情報とを結合し、結合された平文と固定情報とを暗号化し、復号装置において、暗号文を復号する際に、前記固定情報が生成されることにより、暗号文が正しく復号されたと判定する。このように、簡単な方法により鍵の決定ができるという効果がある。

【0118】ここで、前記配布媒体は、さらに、暗号鍵セットに含まれるN個の暗号鍵を用いて固定値からなる固定情報が暗号化されたN個の暗号化固定情報を含み、前記復号方法は、さらに、前記識別番号により識別される1つの暗号化固定情報を読み出す暗号化固定情報読出ステップと、復号鍵セットに含まれる所定数の復号鍵を用いて、前記読み出した暗号化固定情報を復号する暗号化固定情報復号ステップとを含み、前記所定の基準とは、暗号化固定情報を復号して復号文を生成し、生成された復号文に固定値からなる固定情報が含まれることであるように構成してもよい。この方法を用いると、暗号装置において暗号文を生成する際に、さらに固定値からなる固定情報を暗号化して暗号化固定情報を生成し、復

号装置において、暗号文を復号する際に、前記暗号化固定情報が復号されて、固定情報が生成されることにより、暗号文が正しく復号されたと判定する。このように、簡単な方法により鍵の決定ができるという効果がある。

【0119】また、本発明は、配布媒体にデジタルデータを暗号化して書き込んだ暗号装置の種類を識別する鍵管理装置において用いられる鍵管理方法であって、前記配布媒体から1つの暗号化スクランブルキーを読み出す暗号文読出ステップと、1つの復号鍵セットを読み出す復号鍵セット読出ステップと、前記読み出した復号鍵セットに含まれる所定数の復号鍵を用いて、前記読み出した暗号化スクランブルキーを順次復号し、所定の基準により正しく暗号化スクランブルキーを復号する復号鍵を、前記所定数の復号鍵の中から1つ選択する復号選択ステップと、前記配布媒体からN（Nは2以上の整数）個の暗号化スクランブルキーの読み出しが終了するまで、前記暗号文読出ステップ、前記復号鍵セット読出ステップ、前記復号選択ステップに対して、暗号化スクランブルキーの読み出しと、復号鍵セットの読み出しと、読み出した暗号化スクランブルキーの復号とを繰り返すように制御し、この結果、N個の復号鍵のセットが選択される繰返制御ステップと、前記M個の暗号鍵セットから、前記選択されたN個の復号鍵のセットと一致する1つの暗号鍵セットを検出し、検出された暗号鍵セットにより特定される暗号装置の種類を識別する鍵パターン検出ステップとを含む。この方法を用いると、鍵管理装置は、配布媒体がどの種類の暗号装置により生産されたものであるかを識別することができるという効果がある。

【0120】ここで、前記所定の基準とは、前記復号文に固定値からなる固定情報が含まれることであるように構成してもよい。この方法を用いると、暗号装置において暗号文を生成する際に、平文と固定値からなる固定情報とを結合し、結合された平文と固定情報とを暗号化し、復号装置において、暗号文を復号する際に、前記固定情報が生成されることにより、暗号文が正しく復号されたと判定する。このように、簡単な方法により鍵の決定ができるという効果がある。

【0121】ここで、前記配布媒体は、さらに、暗号鍵セットに含まれるN個の暗号鍵を用いて固定値からなる固定情報が暗号化されたN個の暗号化固定情報を含み、前記鍵管理方法は、さらに、N個の暗号化固定情報を読み出す暗号化固定情報読出ステップと、N個の復号鍵セットを用いて、前記読み出したN個の暗号化固定情報を復号する暗号化固定情報復号ステップとを含み、前記所定の基準とは、暗号化固定情報を復号して復号文を生成し、生成された復号文に固定値からなる固定情報が含まれることであるように構成してもよい。この方法を用いると、暗号装置において暗号文を生成する際に、さらに

固定値からなる固定情報を暗号化して暗号化固定情報を生成し、復号装置において、暗号文を復号する際に、前記暗号化固定情報が復号されて、固定情報が生成されることにより、暗号文が正しく復号されたと判定する。このように、簡単な方法により鍵の決定ができるという効果がある。

【0122】

【図面の簡単な説明】

【図1】図1は、本発明に係る1つの実施の形態としての暗号システム10の構成を示すブロック図である。

【図2】図2は、図1に示す暗号システム10の鍵管理装置100の構成を示すブロック図である。

【図3】図3は、図2に示す鍵管理装置100の復号選択部134の構成を示すブロック図である。

【図4】図4は、図2に示す鍵管理装置100の暗号鍵テーブル114と復号鍵テーブル112の構成を示す。

【図5】図5は、図2に示す鍵管理装置100の復号鍵テーブル112の一例を示す。

【図6】図6は、図2に示す鍵管理装置100の暗号鍵テーブル114の一例を示す。

【図7】図7は、図3に示す復号選択部134の復号文生成部143により復号されるスクランブルキーを含む復号文の構成を示す。

【図8】図8は、図1に示す暗号システム10の鍵管理装置100の鍵生成と鍵の配布の動作を示すフローチャートである。

【図9】図9は、図1に示す暗号システム10の鍵管理装置100の暗号装置の種類を特定する動作を示すフローチャートである。

【図10】図10は、図1に示す暗号システム10の暗号装置200の構成を示すブロック図である。

【図11】図11は、図10に示す暗号装置200の鍵暗号化部204の構成を示すブロック図である。

【図12】図12は、図10に示す暗号装置200のデジタルデータ暗号化部202の動作を示すフローチャートである。

【図13】図13は、図10に示す暗号装置200の動作を示すフローチャートである。

【図14】図14は、配布媒体の構成を示す。

【図15】図15は、図1に示す暗号システム10の復号装置300の構成を示すブロック図である。

【図16】図16は、図15に示す復号装置300の復号文生成部306の構成を示すブロック図である。

【図17】図17は、図15に示す復号装置300のデジタルデータ復号部309の動作を示すフローチャートである。

【図18】図18は、図15に示す復号装置300の動作を示すフローチャートである。

【符号の説明】

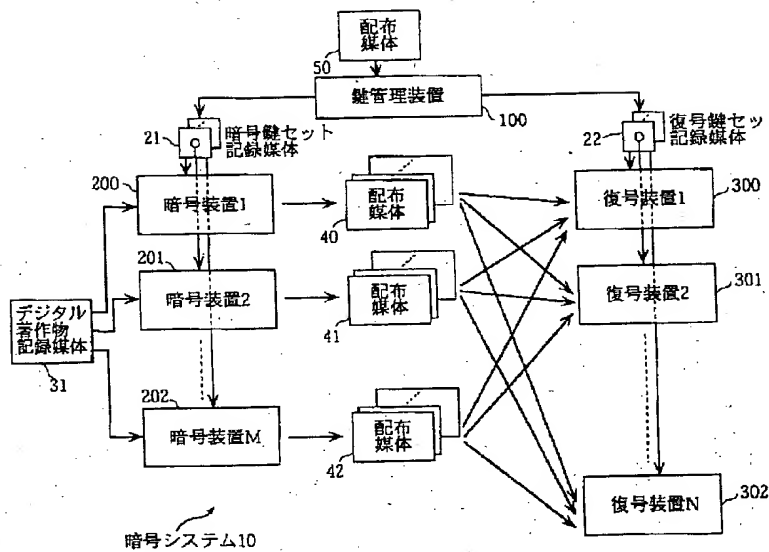
10

暗号システム

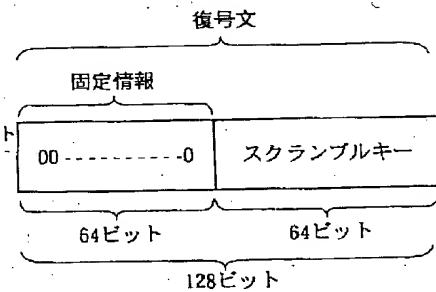
2 1	暗号鍵セット記録媒体
2 2	復号鍵セット記録媒体
3 1	デジタル著作物記録媒体
4 0 ~ 4 2、5 0	配布媒体
1 0 0	鍵管理装置
1 1 1	暗号鍵セット配布部
1 1 2	復号鍵テーブル
1 1 3	暗号鍵生成部
1 1 4	暗号鍵テーブル
1 1 5	暗号鍵生成制御部
1 1 6	暗号鍵セット配布部
1 2 1	識別番号配布部
1 2 2	識別番号記憶部
1 3 1	復号選択制御部
1 3 2	復号鍵セット読出部
1 3 3	暗号文読出部
1 3 4	復号選択部
1 3 5	鍵パターン検出部
1 3 6	暗号装置管理処理部
1 4 1	復号鍵読出部
1 4 2	復号制御部
1 4 3	復号文生成部
1 4 4	復号文検査部

1 4 5	鍵出力部
2 0 0 ~ 2 0 2	暗号装置
2 0 3	スクランブルキー生成部
2 0 4	鍵暗号化部
2 0 5	暗号鍵記憶部
2 0 6	デジタルデータ暗号化部
2 1 1、2 1 4	分解部
2 1 2、2 1 3	D E S 暗号化部
2 1 5	結合部
3 0 0 ~ 3 0 2	復号装置
3 0 3	復号鍵読出部
3 0 4	復号検査制御部
3 0 5	暗号文読出部
3 0 6	復号文生成部
3 0 7	復号文検査部
3 0 8	デジタルデータ読出部
3 0 9	デジタルデータ復号部
3 1 0	表示部
3 1 1	識別番号記憶部
3 1 2	復号鍵記憶部
3 2 1、3 2 4	分解部
3 2 2、3 2 3	D E S 復号部
3 2 5	結合部

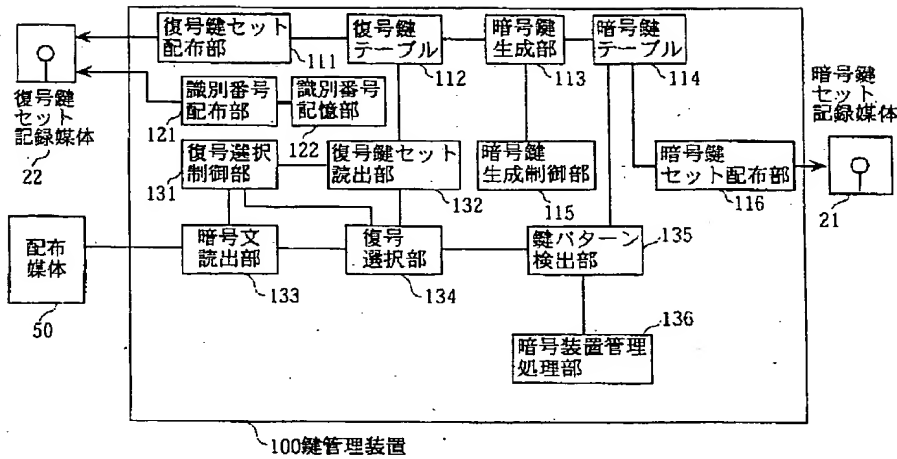
【図 1】



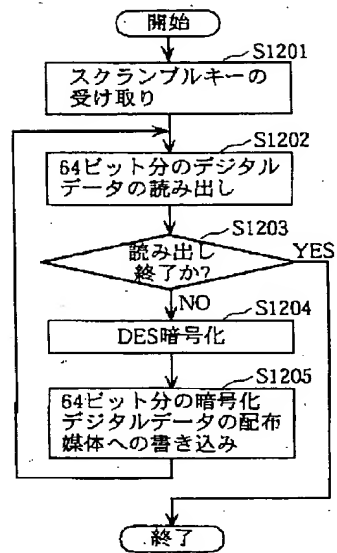
【図 7】



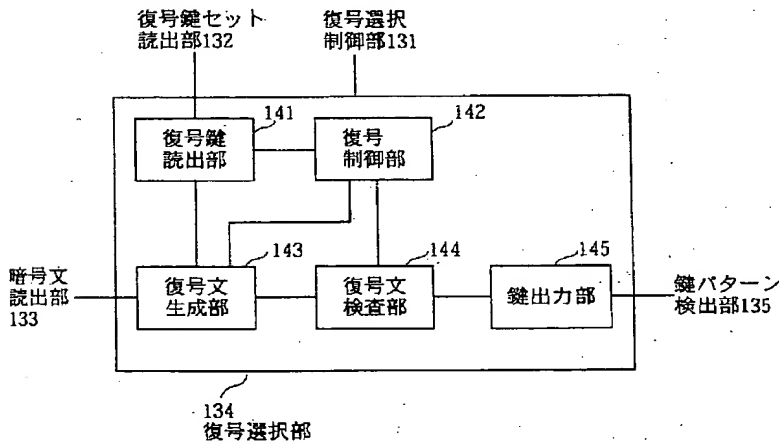
【図2】



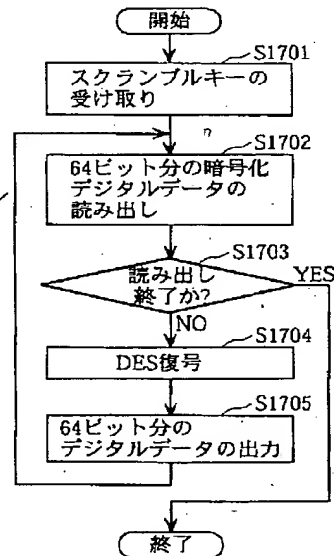
【図12】



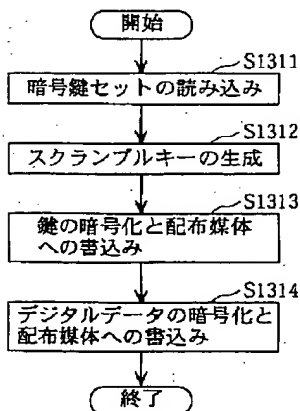
【図3】



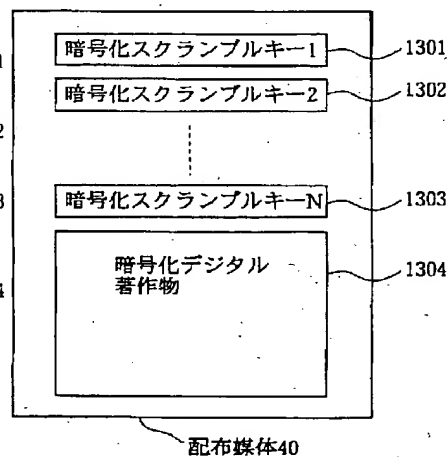
【図17】



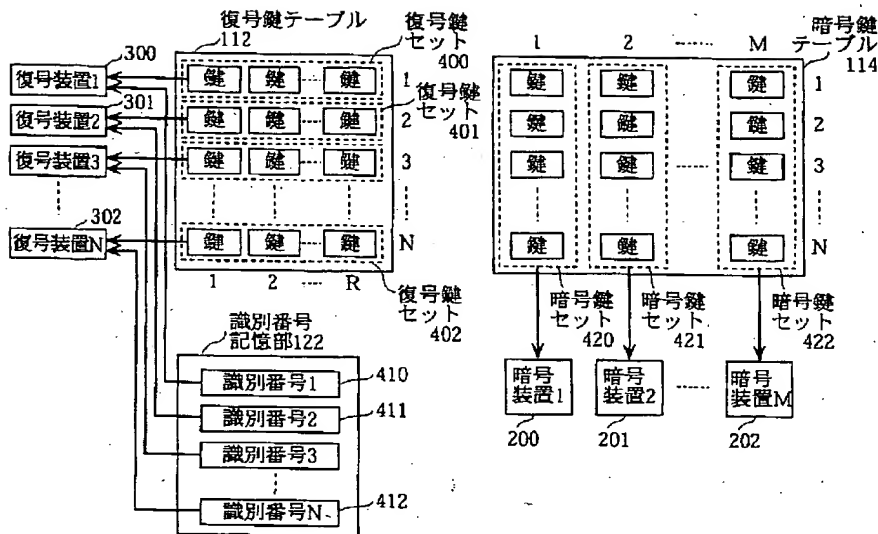
【図13】



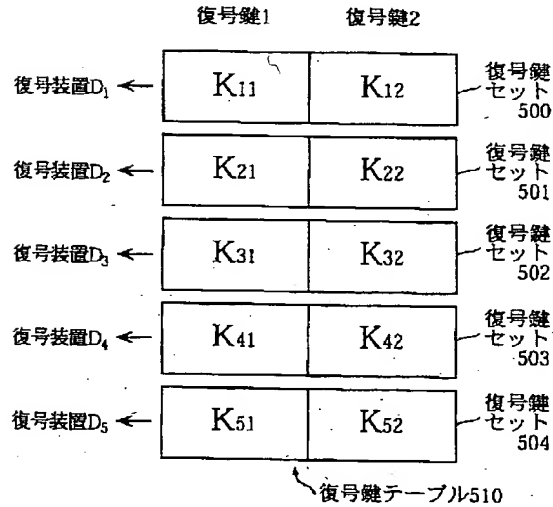
【図14】



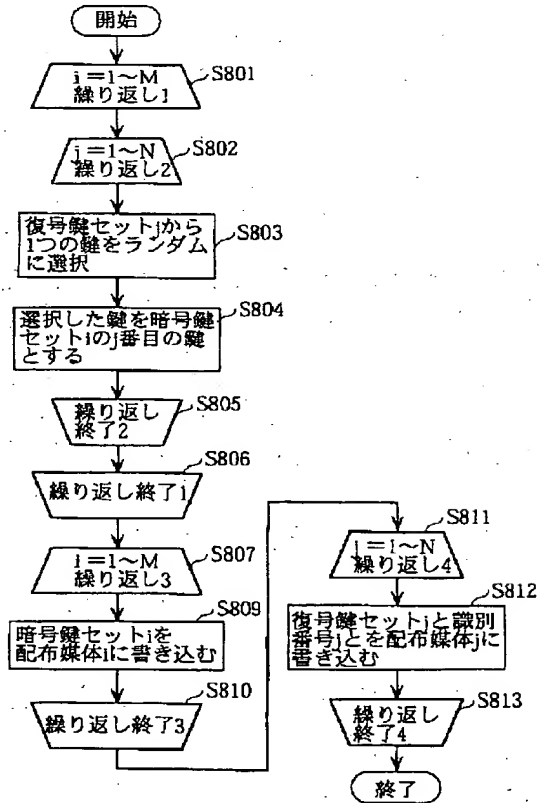
【図4】



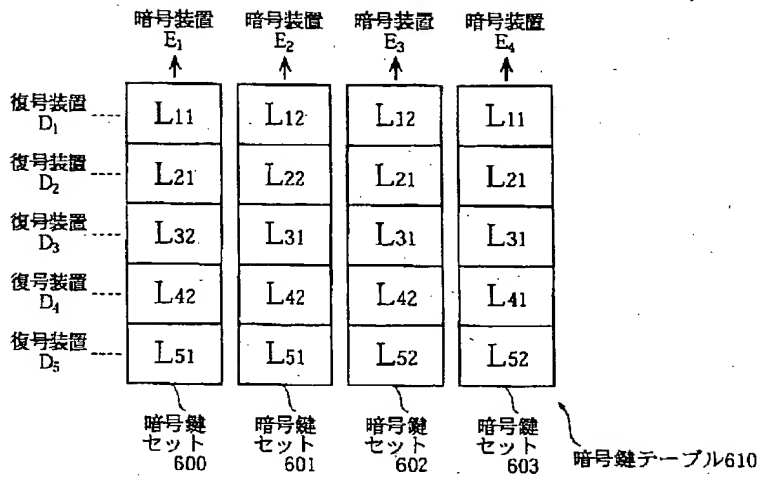
【図5】



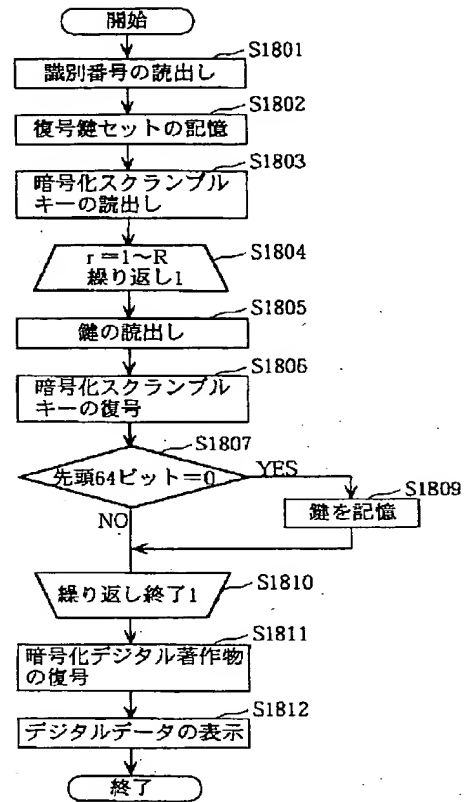
【図8】



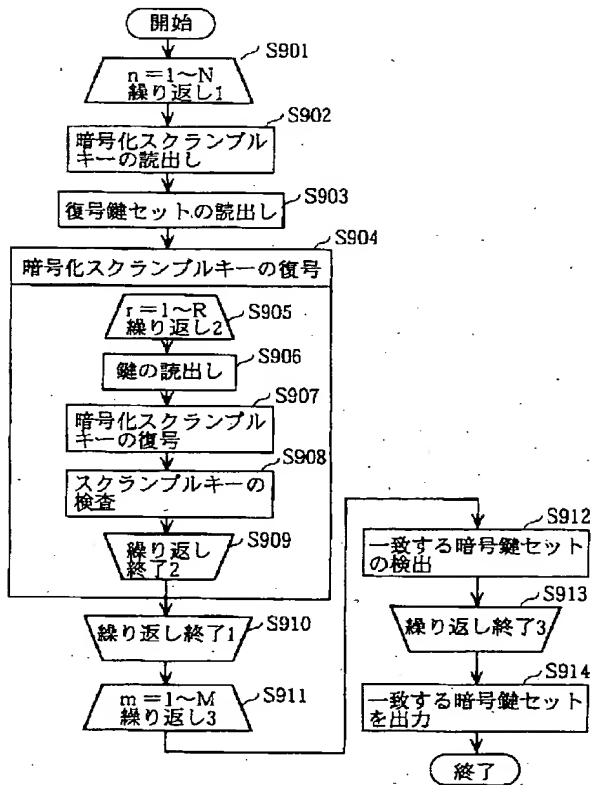
【図6】



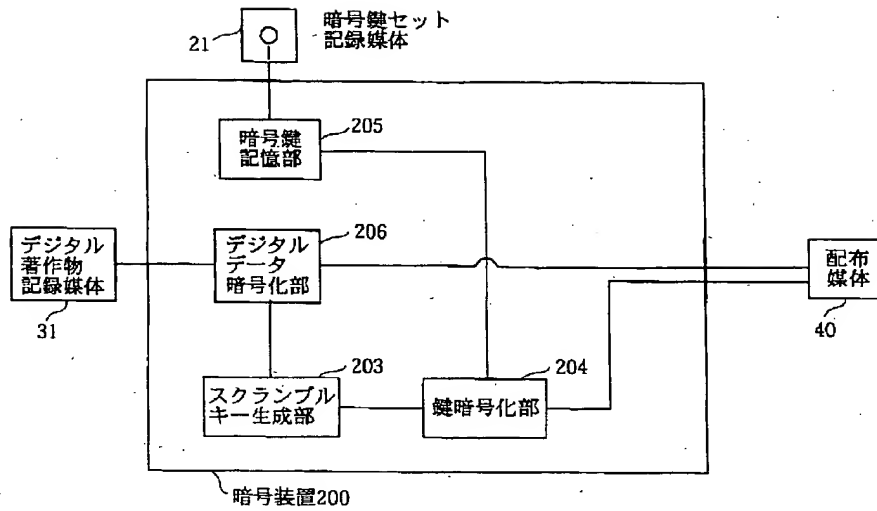
【図18】



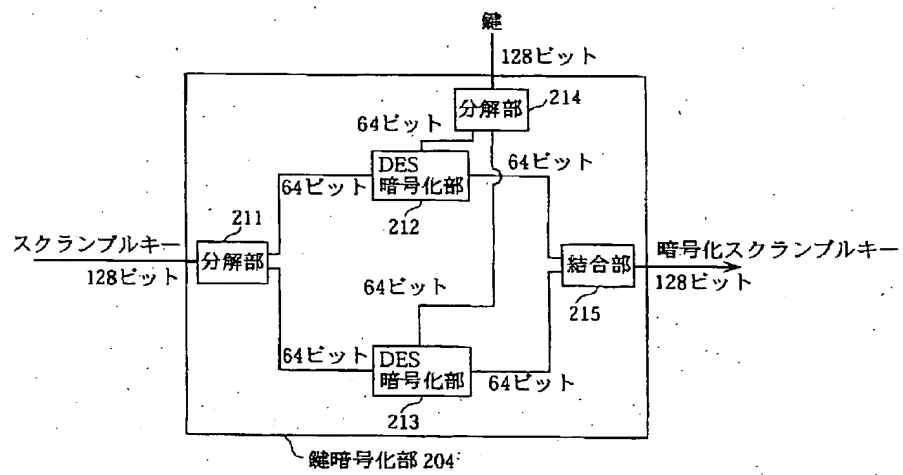
【図9】



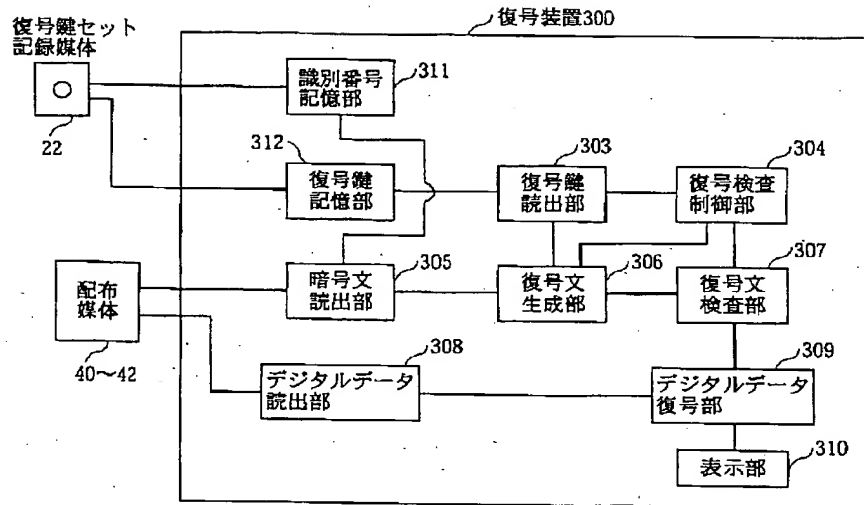
【図 1 0】



【図 1 1】



【図15】



【図16】

